LAHDEN AMMATTIKORKEAKOULU
Lahti University of Applied Sciences

SIIRTYMINEN IPV6-PROTOKOLLAAN YRITYKSEN VERKKOLAITTEISTOSSA

LAHDEN
AMMATTIKORKEAKOULU
Tekniikan ala
Tietotekniikan koulutusohjelma
Tietoliikennetekniikka
Opinnäytetyö
Kevät 2012
Kalle Lindén

Lahden ammattikorkeakoulu
Tietotekniikan koulutusohjelma

LINDÉN, KALLE: Siirtyminen IPv6-protokollaan yrityksen verkkolaitteistossa

Tietoliikennetekniikan opinnäytetyö, 57 sivua

Kevät 2012

TIIVISTELMÄ

Tämän opinnäytetyön tarkoituksena on selvittää, mitä muutoksia Päijät-Hämeen koulutuskonsernin (PHKK) tietoverkon runkolaitteissa tarvitsee tehdä, jotta voidaan ottaa IPv6-protokolla käyttöön. Siirtyminen IPv6-protokollaan tulee olemaan välttämätön toimenpide, koska IPv4-protokollasta loppuvat uudet yksilölliset osoitteet.

IPv4- ja IPv6-protokollien suurimmat erot ovat osoitekentän koon kasvaminen 32 bitistä 128 bittiin. Aluksi IPv4-osoitteistuksessa oli käytössä luokallinen osoitejärjestelmä, mutta osoitteiden tuhlaamisen takia otettiin myöhemmin luokaton IPv4-osoitejärjestelmä. Kun luokattoman osoitejärjestelmän riittämättömyys paikkaamaan osoitteiden loppumisongelmaa huomattiin, otettiin käyttöön osoitteenmuunnos.

Osoitteenmuunnoksen eli NAT:n avulla voidaan piilottaa yhden julkisen IPv4-osoitteen taakse useita päätelaitteita. Ainoa pysyvä ratkaisu on ottaa käyttöön IPv6-protokolla. IPv6-protokollaan siirtymiseen on olemassa eri tekniikoita, kuten dual-stack (IPv4- ja IPv6-protokolla yhtä aikaa toiminnassa), erilaiset tunneloinnit ja osoitteenmuunnos (NAT64) IPv4- ja IPv6-protokollan välillä.

Runkoverkon laitteista valittiin pääasialliseen tarkasteluun palomuurit, reitittimet, kytkimet, langaton järjestelmä sekä DHCP- ja DNS-palvelut. DHCP- ja DNS-palvelut toteutettiin Linux-käyttöjärjestelmään asennetuilla palveluilla.

PHKK:n runkoverkon aktiivilaitteet tukevat kohtuullisen hyvin IPv6-protokollaan siirtymistä. Reitittimien ohjelmisto jouduttiin päivittämään, jotta niihin saatiin tarpeeksi ominaisuuksia, jotta järkevä IPv6-testaus saatiin toteutettua. Linuxin nykyään yleisesti käytössä olevissa kernelin (ytimen) versioissa on IPv6-tuki. ISC:n tekemät DNS- ja DHCP-palvelut tukevat uusimmissa versoissa hyvin IPv6:sta.

Reitittimet, sisäinen palomuuri, kytkimet, langaton järjestelmä sekä DNS- ja DHCP-palvelut saatiin kaikki toimimaan testiympäristössä, jossa käytettiin dual-stack-tekniikkaa. Tämän opinnäytetyön pohjalta voidaan siirtyä turvallisin mielin IPv6-protokollaan.

Asiasanat: TCP/IP, IPv6, Cisco

Lahti University of Applied Sciences
Degree Programme in Information Technology

LINDÉN, KALLE: IPv6 protocol in company network devices

Bachelor's Thesis in Telecommunications, 57 pages

Spring 2012

ABSTRACT

The purpose of this Bachelor's Thesis was to find out what changes need to be done in the core network equipment of the Lahti Region Educational Consortium when taking the new IPv6 protocol for use. The transition to IPv6 protocol is a necessary operation, because new IPv4 addresses will not be granted anymore in the near future.

The main differences between the IPv4 and IPv6 protocols are the increase in the size of address field from 32 bits to 128 bits. There was a classful IP addressing system in the launch of the IPv4 protocol, but due to wasteful usage of addresses, a classless IP addressing system was introduced later. The next step to save IPv4 addresses was network address translation.

The network address translation (NAT) is used to hide many private IPv4 addresses at a single public IPv4 address. The only permanent solution to the IPv4 address exhaustion is the introduction of the IPv6 protocol. There are various techniques for the transition to IPv6 such as dual-stack technology (IPv4 and IPv6 protocols simultaneously in operation) or various tunneling protocols or network address translation from IPv6 to IPv4 addresses (NAT64).

In this study, firewalls, routers, switches, wireless system, DHCP and DNS services were chosen to closer analysis. DHCP and DNS services were running in the Linux operating system.

The Lahti Region Educational Consortium's core network devices support the IPv6 transition reasonably well. Router software had to be updated in order to get enough features to carry out necessary tests. There is IPv6 protocol support in most commonly used Linux kernels. The Internet Systems Consortium provides IPv6 support to their DNS and DHCP services.

Routers, firewall, switches, wireless system, DNS and DHCP services were all successfully made to work in the test environment, which uses dual-stack technology.

Key words: TCP/IP, IPv6, Cisco

SISÄLLYS

LYHENNELUETTELO

ARP	Address Resolution Protocol, IP-osoittetta vastaavaan MAC-osoitteen selvittämiseen tarkoitettu protokolla.
ARPAnet	Advanced Research Projects Agency Network, Yhdysvaltain sotilaallista tutkimusta varten perustettu vuodesta 1983 TCP/IP-protokollaa käyttänyt tietoverkko.
BIND	Berkeley Internet Name Domain, Berkleyn yliopistossa 1980-luvulla kehitetty DNS-palvelin, jota ylläpitää ISC.
CIDR	Classless Inter-Domain Routing, luokaton reititys IPv4-verkkojen jakamiseen alkuperäistä pienempiin osiin käyttäen aliverkonpeitettä.
DHCP	Dynamic Host Configuration Protocol, protokolla IP-osoitteiden jakamiseen päätelaitteille automaattisesti.
DNS	Domain Name System, Internetin nimipalvelujärjestelmä, jolla voidaan muuntaa verkkonimiä IP-osoitteiksi.
DSCP	Differentiated Services Code Point, IP-paketin otsikossa oleva paketin prioriteettiarvo, jota käytetään pakettien priorisoinnissa.
GRE	Generic Routing Encapsulation, tunnelointiprotokolla erilaisten pakettien tunneloimiseen kahden päätepisteen välillä.
HSRP	Hot Standby Router Protocol, Ciscon protokolla reitittimien automaattiseen kahdennukseen.
HTTP	Hypertext Transfer Protocol, yleisin Internetin protokolla, jolla muun muassa www-sivut siirretään.
IANA	Internet Assigned Numbers Authority, Yhdysvalloissa sijaitseva maailmanlaajuinen IP-osoitteiden valvontaelin.

ICMP	Internet Control Message Protocol, TCP/IP-pinon kontrollointiprotokolla viestien nopeaan lähetykseen laitteesta toiseen.
ICT	Information and communications technology, kaikki elektroniset mediat, joita voidaan käyttää apuna tietojenkäsittelyssä.
IMAP	Internet Message Access Protocol, sähköpostin lukemiseen tarkoitettu protokolla.
IP	Internet Protocol, TCP/IP-protokollaperheen IP-tietoliikennepakettien toimittamisesta perille huolehtiva protokolla. IP-protokollalla tarkoitetaan yleensä IPv4-protokollaa.
IPv4	Internet Protocol version 4, vuonna 1981 määritelty versio IP-protokollasta, joka on edelleen laajassa käytössä.
IPv6	Internet Protocol version 6, vuonna 1998 määritelty versio IP-protokollasta, jonka olisi tarkoitus korvata tulevaisuudessa IPv4-protokolla.
IPX	Internetwork Packet Exchange, Novellin NetWare käyttöjärjestelmän käyttämä IP-protokollaa muistuttava protokolla, jota käytettiin enimmäkseen lähiverkoissa.
ISATAP	Intra-Site Automatic Tunnel Addressing Protocol, IPv6-tunnelointiprotokolla päätelaitteiden IPv6-yhteyksien luontiin IPv4-verkon ylitse.
ISC	Internet Systems Consortium, voittoa tekemätön yhtiö pitämään Internetin protokollia laadukkaina ja edullisina.
ISO	International Organization for Standardization, kansainvälinen standardisointijärjestö.
JPEG	Joint Photographic Experts Group, yksi laajimmin tuetuista häviöllistä pakkausta käyttävistä kuvien tallennusformaateista.

L2TP	Layer 2 Tunneling Protocol, Microsoftin ja Ciscon kehittämä OSI-mallin toisella tasolla toimiva VPN-tunnelointiprotokolla.
MAC	Media Access Control, IEEE 802 (esimerkiksi Ethernet) -verkoissa käytetty verkon varaamisen ja liikennöinnin hoitava osajärjestelmä.
MPLS	Multiprotocol Label Switching, menetelmä esimerkiksi IP-pakettien kuljettamiseen ennalta määriteltyjen yhteyksien ylitse nopean runkoverkon solmujen kautta ilman, että solmujen tarvitsee tehdä reititystä.
MTU	Maximum transmission unit, pakettikytkentäisen tietoliikenneverkon yhden paketin suurin koko, joka vaihtelee tekniikan mukaan.
NAPT	Network address port translation, osoitteen ja portin muunnostekniikka julkisten IP-osoitteiden säästämiseksi, joka mahdollistaa yhteen osoitteeseen suuremman piilotetun verkon kuin perinteinen NAT.
NAT	Network address translation, osoitteen muunnostekniikka julkisten IP-osoitteiden säästämiseksi.
PAP	Password authentication protocol, yksinkertainen protokolla salasanojen lähettämiseen, joka lähettää suoraan käyttäjänimen ja salasanan selkokielisenä.
PHKK	Päijät-Hämeen koulutuskonserni -kuntayhtymä, maakunnallinen koulutuksen järjestäjä, kehittäjä ja ylläpitäjä Päijät-Hämeessä.
PPTP	Point-to-Point Tunneling Protocol, PPP-protokollaan perustuva VPN-tunnelointiprotokolla.
RIPE	Réseaux IP Européens, Euroopan paikallinen IP-osoitteiden hallinta elin.
SLAAC	Stateless address autoconfiguration, IPv6-osoitteiden automaattinen generointi reitittimen mainostamaan verkkoon työaseman MAC-osoitteesta.

SOA	Start of Authority, jokaisen DNS-alueen alussa olevat alueen voimassaoloa koskevat määritykset.
SSH	Secure Shell, salattu tietoliikenneprotokolla etäyhteyksien ottamiseen.
TCP	Transmission Control Protocol, tilallinen OSI-mallin neljännen kerroksen tiedonsiirtoprotokolla.
TOS	Type of service, priorisointiin varattu kenttä IPv4 paketissa, johon muun muassa DSCP-arvo sijoitetaan.
TTL	Time to Live, tekniikka IPv4-protokollassa, jolla estetään ikuisten looppien syntymisen tietoliikenneverkkoihin hylkäämällä paketti TTL-arvon saavuttaessa arvon 0.
UDP	User Datagram Protocol, tilaton OSI-mallin neljännen kerroksen tiedonsiirtoprotokolla.
VPN	Virtual Private Network, tapa kahden tai useamman yrityksen verkon yhdistämiseksi tietoturvallisesti julkisen Internetin yli.
VRF	Virtual Routing Table, virtuaalinen reititystaulu useiden erillisten reititystaulujen tekoon, kun ei haluta kaikkien verkkojen reitittyvän keskenään.

1 JOHDANTO

Maailmanlaajuinen tietoverkko Internet jatkaa kasvamistaan. Internet on ollut arkipäivää länsimaissa pidemmän aikaa. Internetin hyödyntäminen erilaisissa käyttökohteissa on yleistynyt ja yritystä, joka ei tarvitse Internetiä mihinkään, on vaikea löytää. Nykyajan verkkoon kytkettävien laitteiden hinnat ovat tulleet niin alas, että kehitysmaissakin alkaa olla vähävaraisemmilla kansalaisilla varaa ostaa laite, jolla pääsee Internetiin.

Verkkoon kytketyt laitteet juttelevat keskenään käyttäen tunnistamiseen IP (Internet Protocol) -osoitteita eikä nimiä, kuten phkk.fi. Nykyään käytössä oleva IPv4 (Internet Protocol version 4) -protokolla on standardisoitu vuonna 1981, jolloin maailmanlaajuisen tietoverkon ei uskottu kasvavan yhtä valtavaksi kuin se on nykyään. IPv4-protokollassa on 32-bittiset osoitteet, jotka mahdollistavat reilu neljä miljardia osoitetta, jotka ovat lähivuosina kaikki käytössä erilaisista osoitteiden säästömekanismeista huolimatta.

IPv4-osoitteiden loppumisen takia on kehitetty uusi protokolla IPv6 (Internet Protocol version 6), jossa on 128 bitin osoitekenttä. Mahdollisia IPv6-osoitteita on noin $3{,}4*10^{38}$, joten tällä kertaa on varauduttu laitteiden räjähdysmäisen kasvun jatkumiseen. IPv6-protokollasta on olemassa standardi jo 1995 vuodelta, mutta koska IPv6 ei ole yhteensopiva IPv4-protokollan kanssa, niin siirtymistä on pitkitetty, koska kustannuksia on haluttu säästää.

Tässä opinnäytetyössä tutustutaan ensin teoriassa IPv4-protokollaan ja siihen, kuinka vanhan protokollan elinikää on onnistuttu pidentämään erilaisilla IPv4-osoitteiden säästömekanismeilla. Sitten tutustutaan IPv6-protokollan toimintaan ja erovaisuuksiin IPv4-protokollan kanssa sekä siirtymävaiheen tekniikoihin. Teorian jälkeen katsotaan, mitä laitteilta vaaditaan, että laitteet toimisivat oikein IPv6-ympäristössä painottuen Päijät-Hämeen koulutuskonsernissa oleviin verkkolaitteisiin. Lopuksi luodaan testiympäristö käyttäen PHKK:n (Päijät-Hämeen koulutuskonserni) verkkolaitteita, joissa testataan IPv6-protokollan toimintaa IPv4-protokollan rinnalla.

Työ tehdään Päijät-Hämeen koulutuskonsernille, ja PHKK tulee käyttämään tämän opinnäytetyön tuloksia hyväksi ottaessaan IPv6-protokollan

tuotantokäyttöön. PHKK on maakunnallinen koulutuksen järjestäjä, kehittäjä ja ylläpitäjä Päijät-Hämeessä. Päijät-Hämeen koulutuskonserniin kuuluu Koulutuskeskus Salpaus, Lahden ammattikorkeakoulu ja Tuoterengas. PHKK:lla on ollut vuonna 2010 päätoimisia opiskelijoita yhteensä noin 12 600, henkilökuntaa noin 1 700, työasemia noin 6300, palvelimia n. 130 ja verkon aktiivilaitteita n. 400.

Työn tavoitteena on selvittää, millaisia muutoksia PHKK:n tietoverkko vaatii, jotta voitaisiin turvallisin mielin ottaa uusi protokolla tuotantoverkon käyttöön. Tässä työssä keskitytään kriittisimpiin verkon osa-alueisiin sisältäen reitittimet, palomuurit, kytkinverkosto, verkon peruspalvelut (DHCP (Dynamic Host Configuration Protocol) ja DNS (Domain Name System)) sekä langaton (WLAN (Wireless Local Area Network)) järjestelmä. Tätä työtä tullaan käyttämään perustana, kun IPv6-protokollaa tullaan ottamaan tuotantokäyttöön. Yhteyttä ulkoverkkoon IPv6-protokollalla ei tässä työssä toteutettu, koska reititys tullaan muuttamaan erilaiseksi ennen kuin IPv6-protokolla otetaan käyttöön.

2 PERUSKÄSITTEET

2.1 Internet

Nykyään Internet on osa jokapäiväistä elämää lähes kaikilla suomalaisilla. Työpaikalla, kotona ja nykyään taskussa matkapuhelimessaan on monella yhteys Internetiin. Internetin kehitys menee nykyään siihen suuntaan, että siitä on tulossa peruspalvelu juoksevan veden ja sähkön rinnalle. 2011 vuonna 89 prosenttia 16-74 vuotiaista käytti Internetiä ja kolme neljästä käytti päivittäin (Suomen virallinen tilasto 2011).

Internet on saanut alkunsa, kun Yhdysvaltojen hallitus havaitsi lamaannuttamattoman verkkotekniikan tarpeellisuuden. Yhdysvallat halusivat kehittää verkoston, jota olisi vaikea lamaannuttaa. Projekti sai nimen ARPA (Advanced Research Projects Agency). (Douglas 2002, 2.)

ARPAnetin kehitys kohti päätavoitetta tehdä lamaantumaton verkko johti siihen, että verkkoon ei tullut keskitettyä hallintapalvelinta, vaan kaikki verkkoon liittyneet koneet olivat samanarvoisia. ARPAnetin toiminta perustui siihen, että viestit pilkottiin pieniin paketteihin, joita verkkolaitteet matkalla päämäärään itsenäisesti ohjasivat eteenpäin, kunnes paketti saavutti päämäärän. (CSC – Tieteen tietotekniikan keskus 1998.)

2.2 OSI-malli

Nykyisten monimutkaisten verkkorakenteiden ymmärtäminen olisi todella haastavaa, jollei olisi kehitetty verkkoliikenteelle kerrosajattelua. Kerrosajattelun ansiosta pysytään verkon toiminnan tarkastelua rajaamaan kerroksittain, joka helpottaa myös vikatilanteiden tarkastelua ja niiden selvittämistä. (Douglas 2002, 177–180.)

Protokollien kerrosrakennetta esittämään on kehitetty kaksi erilaista järjestelmää. Ensimmäinen on ISO:n (International Organization for Standardization) määrittelemä OSI-malli (Reference Model of Open System Interconnection). OSI-mallissa on seitsemän kerrosta, jotka on esitetty kuviossa 1. (Douglas 2002, 181.)

KUVIO 1. OSI-mallin kerrokset (Douglas 2002, 181)

Fyysinen kerros (Physical Layer) määrittää verkon fyysisiä ominaisuuksia. Fyysisiä ominaisuuksia ovat muun muassa standardisoidut johtimet, liittimet, jännite- ja virtatasot. Fyysisellä tasolla toimivia laitteitakin on olemassa. Niissä ei ole mitään älyä, vaan laitteet toistavat samat bitit, jotka laitteeseen tulevat lähteestä. Tällaisia verkkolaitteita ovat esimerkiksi hubit ja toistimet. Yleisin käytössä oleva fyysisen kerroksen protokolla on Ethernet. Fyysinen kerroksen siirtotie voi olla myös langattomasti radioaalloilla toimiva. (Douglas 2002, 182.)

Siirtoyhteyskerros (Data Link Layer) määrittää, miten liikennöidään kahden laitteen välillä. Siirtoyhteyskerroksen tunnetuimpia protokollia on Ethernet. Protokollat voivat siis toimia usealla OSI-mallin tasolla, kuten Ethernet-stantardissa määritellään sekä OSI-mallin ensimmäisen että toisen tason asioita.

OSI-mallin toisella tasolla yleisin verkkolaite on kytkin. Kytkin osaa lukea Ethernet-protokollasta laitteiden MAC (Media Access Control) -osoitteet ja laittaa paketit eteenpäin oikeaan fyysiseen porttiin MAC-osoitteen perusteella. OSI-mallin toisella tasolla käytetään virheentarkistusta, jolla havaitaan siirrossa tapahtuneet virheet (tarkistussumma). (Douglas 2002, 182.)

Verkkokerros (Network Layer) määrittää lähtöpisteestä aina päätepisteeseen asti pakettien reitityksen. Verkkokerroksen verkkolaitteisiin kuuluvat reitittimet. OSI-mallin kolmostason yleisemmin käytetty protokolla on IP (Internet Protocol). IPv6 (Internet Protocol version 6) tulee pitkällä aikavälillä syrjäyttämään vanhan IPv4 (Internet Protocol version 4) tekniikan. IP-protokollan molempia versioita käsitellään myöhemmin omissa kappaleissaan. (Douglas 2002, 182 - 183.)

Kuljetuskerros (Transport Layer) määrittää luotettavan tiedonsiirron lähteestä aina kohteeseen asti. Kuljetuskerros hoitaa pakettien uudelleen järjestelyt, pakettien pilkkomiset, pakettien uudelleen lähetykset ja pakettien ohjauksen kohdepäässä oikealle ohjelmistolle. OSI-mallin neljännen kerroksen toimintaan verkkolaitteet eivät ota kantaa, paitsi palomuurit ja perinteiset palomuuritkin tutkivat vain porttinumeroita eli yrittävät tulkita, mille sovellukselle liikkuva data kuuluu. Kuljetuskerroksen toiminta tapahtuu useimmiten käyttöjärjestelmissä. Yleisimmin käytössä olevat kuljetuskerroksen protokollat ovat TCP (Transmission Control Protocol) ja UDP (User Datagram Protocol). (Douglas 2002, 183.)

Istuntokerros (Session Layer) määrittää mekanismeja istunnon avaamiseen, sulkemiseen ja hallintaan. Istuntokerrosta käytetään muun muassa VPN (Virtual Private Network) -tunneleiden hallintaan. Protokollia, jotka käyttävät istuntokerrosta, ovat esimerkiksi AppleTalk, L2TP (Layer 2 Tunneling Protocol), PAP (Password Authentication Protocol) ja PPTP (Point-to-Point Tunneling Protocol). (Wikipedia 2012.)

Esitystapakerros (Presentation Layer) määrittää sovellusten tarvitsemia toimintoja. Esitystapakerros sisältää rutiineja, jotka voivat esimerkiksi pakata kuvia tai tekstiä ennen siirtoa vastaanottajan ymmärtämään muotoon bittivirroiksi. OSI-mallin kuudennen tason tyypillisempiä käyttökohteita on esimerkiksi JPEG (Joint Photographic Experts Group) -kuvien pakkaus algoritmi. (Douglas 2002, 183.)

Sovelluskerros (Application Layer) määrittää sovellusten käyttämät protokollat. Esimerkkejä protokollista ovat esimerkiksi HTTP (Hypertext Transfer Protocol), SSH (Secure Shell) ja IMAP (Internet Message Access Protocol). (Douglas 2002, 183.)

2.3 TCP/IP-malli

TCP/IP-mallissa on neljä kerrosta, eli kolme vähemmän kuin OSI-mallissa. TCP/IP-malli ei ole minkään standardisointikomitean laatima, vaan TCP/IP-protokollaperheen tutkimisen tuloksena syntynyt malli. (Hakala & Vainio 2005, 183.)

KUVIO 2. TCP/IP-mallin vertailu OSI-malliin (Hakala & Vainio 2005, 184)

TCP/IP-viitemallin alin kerros on kuvion 2 mukaisesti peruskerros (Link Layer). Peruskerros sisältää OSI-mallin kaksi alinta kerrosta. TCP/IP-mallissa peruskerroksen tehtävänä on siirtää paketti kahden pisteen välillä. TCP/IP-mallissa ei oteta kantaa, miten paketti siirtyy kahden solmun välillä, ja mallissa oletetaan, että taustalla on olemassa toimivat fyysiset yhteydet ja protokollat siirtää paketteja solmupisteiden välillä. (Douglas 2002, 185.)

TCP/IP-mallin verkkokerros (Internet Layer) vastaa hyvin pitkälle OSI-mallin verkkokerrosta. Verkkokerroksesta on käytetty myös nimitystä Internet-kerros. Verkkokerroksessa nykyisin yleisin protokolla on IPv4. Verkkokerros hoitaa pakettien kapseloinnin IP-tietosähkeeseen, lähettää paketin eteenpäin reitititysalgoritmien avulla joko toiseen verkkoon tai ylemmille mallin tasoille.

Verkon diagnostiikkaan liittyvät ICMP (Internet Control Message Protocol) -protokollaan perustuvat toiminnot kuuluvat verkkokerrokseen. (Douglas 2002, 185.)

Kolmas kerros TCP/IP-mallissa on kuljetuskerros (Transport Layer). Kuljetuskerroksen tärkeimpiin tehtäviin kuuluu pakettien ohjaus oikeille sovelluksille ja datan pilkkominen pieniin paketteihin. Kuljetuskerros voi myös huolehtia ruuhkan hallinnasta, pakettien virheettömyyden tarkistuksesta päästä päähän yhteyksissä ja pakettien oikeasta järjestyksestä. Kuljetuskerros vastaa täysin OSI-mallin kuljetuskerrosta. Kolmannen kerroksen yleisimmät käytössä olevat protokollat ovat TCP ja UDP. (Douglas 2002, 184–185.)

TCP/IP-mallin ylin kerros eli sovelluskerros (Application Layer) yhdistää OSI-mallin istunto-, esitystapa- ja sovelluskerrokset. Sovelluskerrokseen kuuluvat TCP/IP-verkkoa hyödyntävät sovellukset ja palvelut. TCP/IP-malli ei ota kantaa sovellusten toiminnallisuuksiin, vaan olettaa, että sovellukset siirtävät tiedot oikeassa muodossa kuljetuskerrokseen tietojen kuljettamista varten. (Douglas 2002, 184.)

3 IPV4-PROTOKOLLA

Kuten aiemmin todettiin, IPv4 on nykyään verkkokerroksen hallitseva protokolla. IPv4 on hyvin toimiva protokolla, jonka suurin heikkous on sen IP-osoitteiden loppuminen. IP-osoitteiden tärkeys on verrattavissa puhelinnumeroihin. Verkkokerroksen protokollien tarkoitus on reitittää pakettipohjainen liikenne läpi pakettikytkentäisen verkon aina perille asti.

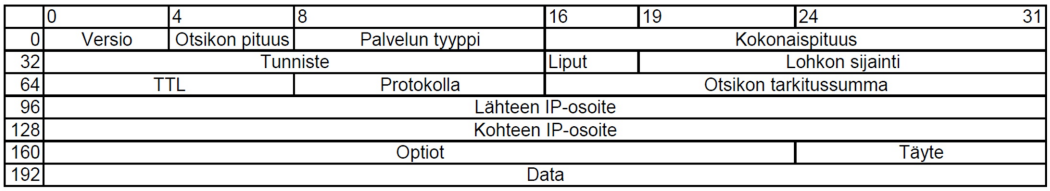
IPv4 on yhteydetön pakettien kuljetusprotokolla. Protokolla on epäluotettava, sillä se ei sisällä minkäänlaista mekanismia, jolla se varmistaisi pakettien perille pääsyn. Paketit kulkevat Internetin läpi reitittimien kautta. Jokainen reititin toimii itsenäisesti ohjaten paketteja reititystaulun mukaisesti. Reititystaulu voi olla dynaamisesti muodostettu, jonkun reititysprotokollan muodostamana. Reititystauluun voi myös käsin kiinteästi määrätä kohde IP-osoitteen perusteella, minne paketti seuraavaksi kuuluisi lähettää. Samasta päätelaitteesta samaan kohteeseen lähteneet paketit voivat siis mennä eri reittiä kohteeseen. Tämä aiheuttaa sen, että osa paketeista saattaa viipyä reitillä pidempään, jolloin ensimmäiseksi lähetetty paketti tuleekin myöhemmin perille kuin myöhemmin lähetetyt paketit. Paketteja saattaa myös hävitä matkalla esimerkiksi verkon ruuhkaisuuden takia. (Douglas 2002, 97.)

IPv4-protokollasta on haluttu tehdä yhteydetön ja epäluotettava, koska tällöin reitittimien toiminta muuttuu paljon yksinkertaisemmaksi. Reitittimien ei tarvitse huolehtia pakettien koko matkasta vaan ainoastaan reititystaulun perusteella lähettää paketit parhaansa mukaan eteenpäin. Operaattoreiden runkoverkkojen reitittimien lävitse kulkee valtava määrä paketteja, jolloin on teknisesti järkevämpää käyttää kuljetuskerroksen protokollaa pitämään huolta pakettien perille menosta ja oikeasta järjestyksestä. Kuljetuskerroksen toiminta kuluttaa resursseja päätelaitteilta, jolloin reitittimien resurssit jäävät verkkokerroksen protokollien käyttöön.

3.1 IPv4-protokollan otsikko

Kuviossa 3 on esitetty IPv4-paketin otsikon rakenne. Ensimmäiset 4 bittiä kertovat, että kyseessä on versionumeroltaan 4 oleva IP-paketti. Kentällä halutaan

varmistaa, että kaikki paketin kulkuun osallistuvat laitteet osaavat lukea otsikkotietoja oikein. Seuraava neljän bitin kenttä kertoo otsikon pituuden. Otsikon pituus voi vaihdella viimeisenä kenttinä olevien optioiden ja täytteen mukaan. (Douglas 2002, 98 - 99.)



KUVIO 3. IPv4-tietosähkeen otsikkorakenne (Douglas 2002, 98)

Kokonaispituuskenttä kuvion 3 mukaistesti kertoo IPv4-paketin kokonaispituuden. Kenttä on 16 bittiä pitkä. Tämä rajoittaa IPv4-paketin suurimmaksi mahdolliseksi pituudeksi 2^{16} eli 65 535 tavua. Palvelun tyyppi -kentästä voidaan käyttää myös nimitystä TOS (type of service). TOS-kentällä kerrotaan reitittimille, millaista palveluntasoa kyseiselle paketille halutaan. Tällä voidaan vaikuttaa reitittimessä järjestykseen, jossa paketit käsitellään. Tätä ominaisuutta eivät kuitenkaan kaikki reitittimet tue, joten palveluntaso kentällä ei voida taata haluttua palveluntasoa. Kentän kuusi ensimmäistä bittiä muodostavat DSCP (Differentiated Services Code Point) -arvon, jolla paketteja voidaan priorisoida. (Douglas 2002, 99 - 100.)

IPv4-paketilla on olemassa elinikä. Paketin eliniällä estetään paketin joutumisen ikuiseen looppiin esimerkiksi reititystaulujen virheellisyyksien kautta. Tätä varten IPv4-paketin otsikkoon on laitettu 8 bittiä pitkä elinikä-kenttä. Jokainen matkalla oleva reititin vähentää TTL-arvosta (Time To Live) yhden. Kun TTL-arvo saavuttaa nollan, paketti hylätään ja lähettäjälle lähetetään ICMP-protokollaa käyttäen virheviesti. (Douglas 2002, 106.)

Protokolla-kenttä kertoo, mikä protokolla paketin kuljetuskerroksella on käytössä. Protokolla-kentän arvosta riippuen vastaanottaja osaa olettaa, millä protokollalla IPv4-paketin DATA-osaa tulisi lukea. Otsikon tarkistussumma-kenttä sisältää 16-bittisen tarkistussumman otsikolle. IPv4-protokollassa tarkistetaan pelkästään otsikon eheys, joten hyötydatan eheyden tarkistus jää ylemmille protokollille. (Douglas 2002, 107.)

IPv4-paketin kehykseen täytyy lähettäjän määritellä lähde- ja kohde-ip-osoitteet. Paketin otsikossa olevat IP-osoitetiedot pysyvät samana lähettäjältä vastaanottajalle, paitsi jos jossain käytetään osoitteenmuunnosta, jolla voidaan piilottaa useampi päätelaite yhden IP-osoitteen taakse. Globaalit IPv4-osoitteet ovat yksilöllisiä 32 bittiä pitkiä numerosarjoja. (Douglas 2002, 107.) IP-osoitteista kerrotaan myöhemmin lisää.

TCP/IP-mallin peruskerroksella voi olla useita eri tekniikoita yhdenkin paketin siirrossa paikasta lähteestä kohteeseen. Peruskerroksen tekniikoissa voi suurimman mahdollisen paketin koko vaihdella. Suurimmasta mahdollisesta paketinkoosta käytetään nimitystä MTU (Maximum Transfer Unit). Esimerkiksi jos lähetettävän työasema on kytketty Ethernet-lähiverkkoon, tällöin MTU on 1500 tavua. Mikäli paketti joutuisi matkan varrella, esimerkiksi reitittimien välillä, kulkemaan verkossa, jonka MTU on 620 tavua, joudutaan paketti pilkkomaan 1500 / 620 = kolmeksi eri paketiksi. Pilkottuja paketteja kutsutaan lohkoiksi. Paketteja, jotka on pilkottu useammaksi lohkoksi, ei koota matkanvarrella uudestaan isommaksi paketiksi, vaan paketit kuljetetaan lohkoina perille asti. (Douglas 2002, 102 - 103.)

IPv4:n kehyksessä olevat tunniste-, liput- ja lohkon sijainti -kentät auttavat lohkottujen pakettien hallinnassa. Tunniste-kentällä lähettäjä yksilöi paketit. Samalla tunnisteella samasta lähdeosoitteesta tulleet useammat paketit ovat siis lohkottu matkalla. Liput-kentässä käytetään kolmesta bitistä kahta alempaa. Toiseksi alin bitti on *don't fragment* -bitti. Tämä tarkoittaa, että kyseistä IP-pakettia ei saa lohkota. Mikäli paketti, jossa on *don't fragment* -bitti asetettuna ja kyseisen paketin pitäisi mennä verkkoon, jonka MTU on pienempi kuin paketin koko, reititin hylkää paketin ja lähettää virhesanoman lähettäjälle. Alin bitti on *more fragments* -bitti. Mikäli *more fragments* -bitti on asetettuna, tällöin vastaanottaja tietää, että lisää lohkoja on vielä tulematta, joten alkuperäistä pakettia ei voida vielä koota. Lohkon sijainti -kentällä kerrotaan, missä kohtaa alkuperäistä pakettia kyseinen lohko sijaitsee. (Douglas 2002, 104 - 106.)

Internet Protocol version 4 kehyksessä on vielä määritelty optiot-kenttä. Kenttää ei tarvita normaalisti, mutta sitä voidaan käyttää verkon testaamisessa ja

vianmäärityksessä. Optiot-kentän pituus vaihtelee valittujen optioiden mukaan. (Douglas 2002, 107.)

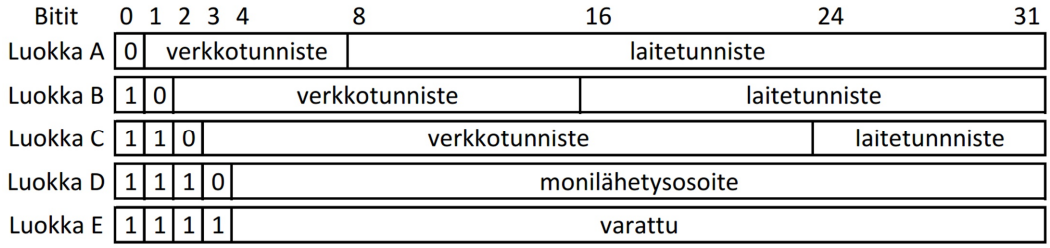
3.2 Osoitteistus

IP-osoitteilla voidaan useat verkot saada näyttämään yhdeltä isolta verkolta. IP-osoitteissa on tehty tietty logiikka reititystä helpottamaan. IP-osoitteessa on aina verkko-osa ja laiteosa. Laiteosasta voidaan käyttää myös nimitystä työasemaosa. Aikoinaan IP-protokollaa suunnitellessa ei osattu ottaa huomioon tulevan Internetin suosion räjähdysmaista kasvua. Alkuperäisessä luokallisessa jaottelussa IP-osoitteet jaettiin luokkiin, joissa oli kolme erilaista luokkaa unicast eli täsmälähetysosoitteille. Osoitteilla oli luokan mukaan tietty osa verkko-osaa ja tietty osa oli laiteosa. (Douglas 2002, 64.)

Binäärimuoto	1100 0000	1010 1000	0000 0001	0110 0100
Desimaalimuoto	192.	168.	1.	100

KUVIO 4. IPv4-osoitteen esitysmuodot (Douglas 2002, 69)

Todellisuudessa fyysisellä tasolla on jännitetasoja, jotka vastaavat digitaalisessa tiedonsiirrossa joko arvoa ”1” (yksi) tai ”0” (nolla). IPv4-osoite on siis 32-bittinen, eli siinä on 32 ”ykköstä ja nollaa” peräkkäin. Ihmisille lukemista ja asetusten määritystä varten osoitteet on muutettu desimaalimuotoon kuvion 4 mukaisella tavalla. Osoite esitetään desimaalimuodossa neljänä pisteillä erotetuilla kokonaisluvuilla, joista jokainen osa on yhden oktetin eli tavun pituinen. (Douglas 2002, 69.)



KUVIO 5. Luokallinen IPv4 osoitejako (Douglas 2002, 64)

Kuviossa 5 on esitetty luokallisten IP-osoitteiden jakautuminen. IP-osoitteen ensimmäiset bitit kertovat verkkolaitteille, mistä luokasta on kyse. D-luokka on tarkoitettu monilähetysosoitteille, joita kutsutaan multicasteiksi. (Douglas 2002, 64.)

	Alin osoite	Ylin osoite	verkko-osa	työasemaosa	vekkoja	työasemia verkossa
Luokka A	1.0.0.0	126.0.0.0	a.	b.c.d	2^{7}=128	2^{24}=16 777 216
Luokka B	128.1.0.0	191.255.0.0	a.b.	c.d	2^{14}=16 384	2^{16}=65 536
Luokka C	192.0.1.0	223.255.255.0	a.b.c.	d	2^{21}=2 097 152	2^{8}=256
Luokka D	224.0.0.0	239.255.255.255	ei määritetty (multicast)			
Luokka E	240.0.0.0	255.255.255.254	ei määritetty			

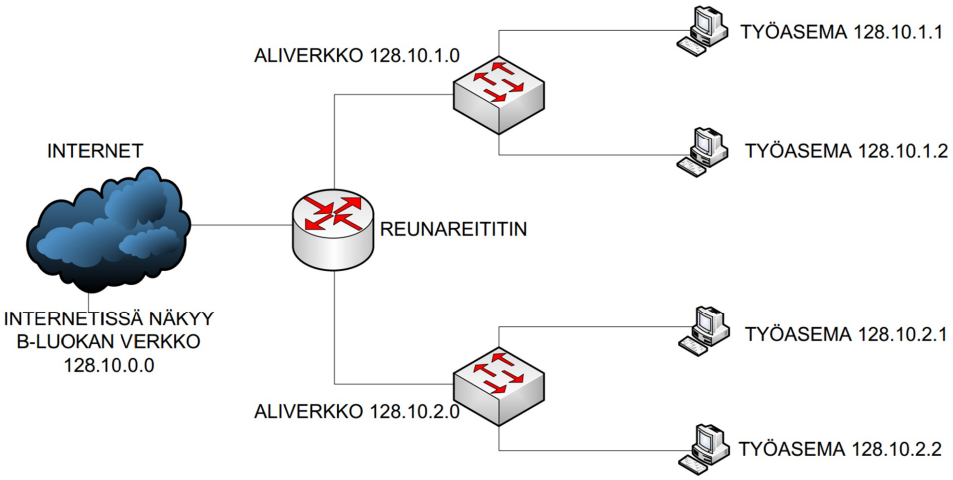
KUVIO 6. IPv4 luokallisten verkkojen osoiteavaruudet ja verkkojen koot (Douglas 2002, 70)

Luokallisten IPv4-osoitteiden jakautuminen kuvion 6 mukaisiin osoiteavaruuksiin tulee siitä, kun kuvion 5 mukaiset ensimmäiset bitit osoitteessa muutetaan desimaalimuotoon. Luokallinen IPv4-osoitejako on yksinkertainen ja helppo toteuttaa ja ymmärtää, mutta sillä on myös heikkouksia. (Douglas 2002, 65.)

Luokallinen IP-osoitejako tuhlaa osoitteita, kun verkkojen kokoja ei voi määrittää todellisen tarpeen mukaan. Esimerkiksi jos käytetään kahden reitittimen välistä linkkiverkkoa, johon tarvitaan kaksi osoitetta, eli molemmille reitittimille oma, on pienin verkko C-luokka. Jos C-luokasta ottaa 2 osoitetta käyttöön ottaen huomioon broadcast- ja verkko-osoitteen huomioon, tällöin tarvitaan tällaiseen linkkiverkkoon yhteensä 4 osoitetta. C-luokan verkossa on 256 osoitetta, jolloin menee 256 - 4 = 252 osoitetta hukkaan.

Luokallisten IP-osoitteiden isoista verkkokokojen portaista tuli ongelma, kun Internetin suosio jatkoi kasvamistaan. IP-osoitteiden tuhlaamiseen piti keksiä

järjestelmä, jolla verkkojen kokoja voitaisiin kasvattaa ja pienentää huomattavasti pienemmissä portaissa.



KUVIO 7. Aliverkko-osoitejärjestelmä (Douglas 2002, 152)

Ensimmäinen askel käytettävien IP-osoitteiden lisäämisessä oli aliverkko-osoitejärjestelmä. Tämä mahdollisti asiakkaalle annetun esimerkiksi B-luokan osoiteavaruuden jakamiseen useampaan osaan asiakkaan omassa reitittimessä kuvion 7 mukaisesti. Tällöin asiakkaan ei tarvinnut varata kahta B-luokkaa, vaan asiakas pystyi omassa reitittimessään aliverkottamaan isomman osoitelohkon pienemmiksi verkoiksi. Internetin runkoreitittimet eivät tiedä näistä aliverkoista, vaan ainoastaan reunareititin. Tämä tekniikka toi osoitteiden loppumiseen pientä ensihätää, eikä Internetin runkoreitittimiin tarvinnut tehdä juuri mitään muutoksia. (Douglas 2002, 152.)

Aliverkko-osoitejärjestelmä ei riittänyt vastaamaan alati kasvavaan tarpeeseen uusille IP-osoitteille. Ratkaisuksi kehitettiin vielä nykyäänkin laajassa käytössä oleva luokaton osoitejärjestelmä, josta voidaan käyttää myös nimitystä yliverkottaminen ja joissain lähteissä käytetään myös nimitystä aliverkottaminen. Luokattomassa järjestelmässä ei enää pystytä päättelemään suoraan IP-osoitteesta, mitkä bitit kuuluvat verkko- ja mitkä laiteosaan. Luokattomassa osoitejärjestelmässä on osoitteen lisäksi tiedettävä myös 32-bittinen aliverkonpeite tai toiselta nimeltään maski. Aliverkon peite kertoo, kuinka monta bittiä osoitteesta kuuluu verkko-osaan ja kuinka monta laiteosaan. Luokattomassa järjestelmässä tulee bitit olla peräkkäin, eli toisin sanoen aliverkonpeite kertoo

kuinka monta bittiä alusta alkaen osoitteesta kuuluu verkko-osaan. (Douglas 2002, 164 - 165.)

TAULUKKO 1. IPv4 aliverkon peitteet listattuna.

CIDR-muoto	Desimaalimuoto	Osoitteita verkossa	CIDR-muoto	Desimaalimuoto	Osoitteita verkossa
/32	255.255.255.255	1	/16	255.255.0.0	65 536
/31	255.255.255.254	2	/15	255.254.0.0	131 072
/30	255.255.255.252	4	/14	255.252.0.0	262 144
/29	255.255.255.248	8	/13	255.248.0.0	524 288
/28	255.255.255.240	16	/12	255.240.0.0	1 048 576
/27	255.255.255.224	32	/11	255.224.0.0	2 097 152
/26	255.255.255.192	64	/10	255.192.0.0	4 194 304
/25	255.255.255.128	128	/9	255.128.0.0	8 388 608
/24	255.255.255.0	256	/8	255.0.0.0	16 777 216
/23	255.255.254.0	512	/7	254.0.0.0	33 554 432
/22	255.255.252.0	1 024	/6	252.0.0.0	67 108 864
/21	255.255.248.0	2 048	/5	248.0.0.0	134 217 728
/20	255.255.240.0	4 096	/4	240.0.0.0	268 435 456
/19	255.255.224.0	8 192	/3	224.0.0.0	536 870 912
/18	255.255.192.0	16 384	/2	192.0.0.0	1 073 741 824
/17	255.255.128.0	32 768	/1	128.0.0.0	2 147 483 648

Aliverkonpeitteen voi esittää kahdella eri tavalla. Toinen vaihtoehto on IP-osoitteen jälkeen kauttaviivalla ilmaistuna. Kauttaviiva ilmaisusta käytetään myös nimitystä CIDR-muoto. Kauttaviivan jälkeinen luku ilmoittaa, kuinka monta bittiä osoitteen alusta lähtien kuuluu verkko-osaan. Taulukossa 1 on lueteltu mahdolliset aliverkon peitteet sekä CIDR- että desimaalimuodossa. Desimaalimuodossa bitit on laskettu yhteen samalla tavalla kuin IP-osoitteissa. Desimaalimuoto on huomattavasti yleisempi tapa ilmoittaa aliverkonpeite. (Douglas 2002, 166.)

3.3 NAT- Network Address Translation

NAT (Network Address Translation) -tekniikka on lisännyt ja lisää edelleen IPv4-protokollan elinikää. NAT-tekniikalla voidaan yhden Internetiin julkisen IP-osoitteen taakse piilottaa useita verkkoon liitettyjä laitteita. NAT-tekniikka on yleisemmin käytössä kotiverkoissa ja yritysten työasemaverkoissa. Osa Suomen operaattoreista on siirtynyt käyttämään mobiiliverkoissaan NAT-tekniikkaa.

NAT-osoitteenmuunnos tehdään useimmiten palomuurissa tai reunareitittimessä mahdollisimman lähellä Internet-rajapintaa. Sisäverkossa laitteille on annettu privaattiosoitteet (privaattiverkot: 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/24). Näitä privaattiverkkojen osoitteita ei Internetissä reititetä. NAT-laiteella on

olemassa yksi tai useampi ulkoverkon (Internet kelpoinen) IP-osoite. NAT-laite muuntaa IP-paketin lähde osoitteen vastaamaan ulkoverkon osoitetta ja päivittää omaan tietokantaansa, että kun ulkoverkon IP-osoitteeseen tulee vastaus, niin tälle paketille tehdään osoitteenmuunnos toisinpäin, eli muutetaan kohdeosoite ulkoverkon osoitteesta sisäverkon osoitteeksi. (Douglas 2002, 394 - 397.)

Perinteinen NAT-osoitteenmuunnos ei toimi kovin hyvin, koska työasemat arpovat portin, josta lähettävät IP-paketin, ja mikäli useampi kone ottaa yhteyden samasta portista, ei NAT-laite enää tiedä, mille sisäverkon laitteelle vastauspaketti kuulusi toimittaa. Tämä ongelma on kierretty NAPT (Network Address Port Translation) -tekniikalla. NAPT-tekniikassa NAT-laite vaihtaa osoitteen lisäksi lähdeportin, jolloin jokainen yhteys on varmasti eri portista NAT-laitteen valitsemana. NAPT-tekniikka kasvattaa perinteiseen NAT-tekniikkaan verrattuna kuormitusta NAT-laitteessa. (Douglas 2002, 396 - 397.)

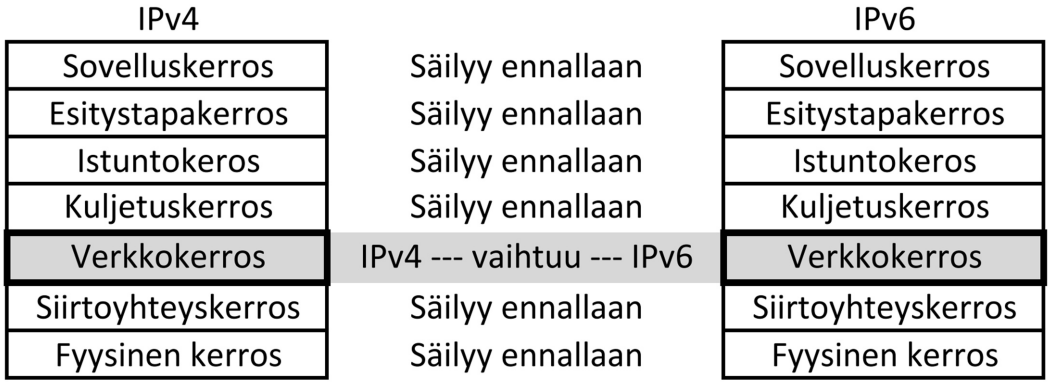
NAT-tekniikka sisältää ongelmia, jotka puoltavat IPv6-protokollaan siirtymistä. NAT-tekniikka rikkoo IP-protokollan alkuperäisen toimintatavan, jossa IP-pakettien tietosisältöihin (OSI mallissa tasolta kolme ylöspäin) oli tarkoitus puuttua vain paketin lähde- ja kohdelaiteissa. Toinen ongelma liittyy verkon suorituskyvyn huonontumiseen. NAT-laite vaatii laskentatehoa, kun sen tarvitsee muuntaa IP-osoitteet ja portit sekä laskea uudelleen IP-paketin tarkistussumman osoitteiden vaihtuessa. Lisäksi tietokantaan täytyy olla merkattuna jokaisen yhteyden tila, julkiset ja privaatit IP-osoitteet ja julkiset ja privaatit portit. Kapasiteettia tarvitaan aina vain lisää, kun laitteet, yhteyksien määrä ja Internet-kaistan nopeus kasvaa.

Ongelmaksi voi myös muodostua, kun haluttaisiin jäljittää IP-osoitteen perusteella, kuka on liikennöinyt Internetissä kyseisellä osoitteella, koska kyseinen julkinen osoite on voinut olla käytössä useilla sadoilla työasemilla. Päätelaitteeseen, joka on NAT-laitteen takana, ei voida ottaa yhteyttä Internetistä, koska kun julkiseen IP-osoitteeseen tulee IP-paketti, ei NAT-laite tiedä, mille sisäverkon päätelaitteelle kyseinen paketti on tarkoitettu. Viimeisenä isompana ongelmana voidaan mainita organisaatioiden tai yritysten liittoutuessa ja verkkojen yhdistämisessä voi käydä niin, että molemmilla organisaatioilla on

käytössä samat sisäverkon IP-osoitteet, jolloin jommankumman on muutettava osoitteet toisiin. (Desmeules 2007, 13 - 15.)

4 IPV6-PROTOKOLLA

IPv6-protokollan tehtävä on tulevaisuudessa korvata IPv4 kokonaan. IPv6-protokolla ei ole yhteensopiva IPv4-protokollan kanssa, minkä takia korvaaminen tapahtuu pitkällä aikavälillä, koska vanhemmat laitteet ja sovellukset eivät tue IPv6:ta. Siirtyminen tulee olemaan työläs, mutta pakollinen prosessi. IPv6-protokollan 128-bittinen osoiteavaruus on niin laaja, että tuskin enää ikinä tarvitsee osoitteiden loppumisen takia vaihtaa ISO:n OSI-mallin kolmannen tason protokollaa. Siirtyessä IPv4:sta IPv6 protokollaan, muihin OSI-mallin tasoihin ei tarvitse tehdä muutoksia kuvion 8 mukaisesti.



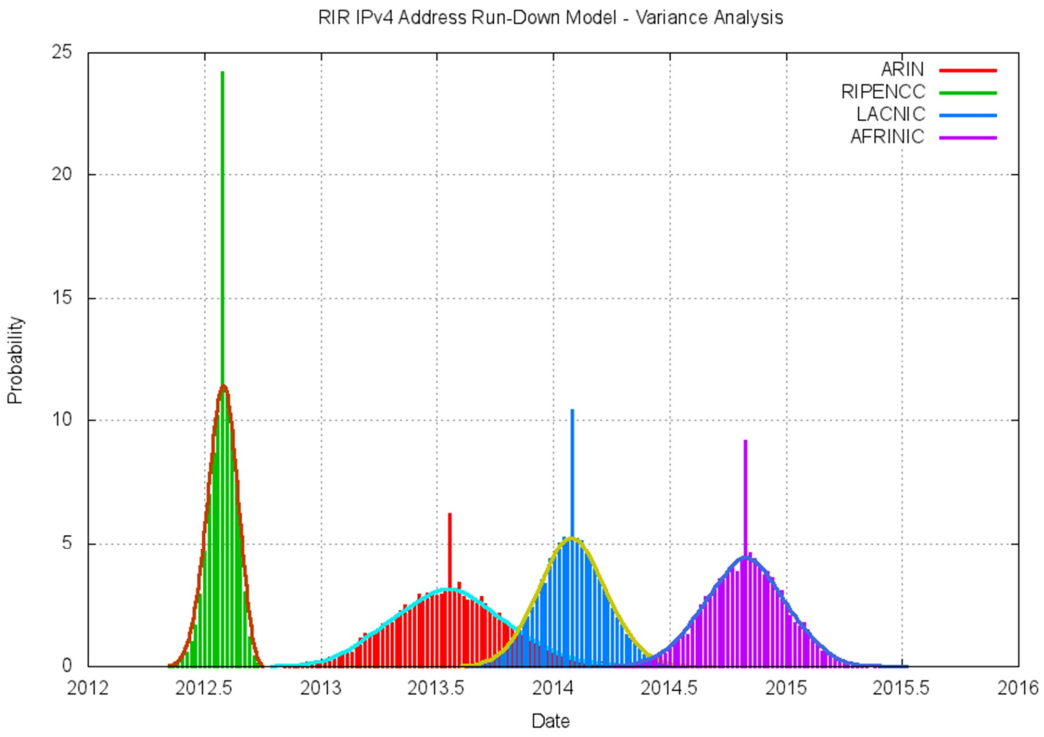
KUVIO 8. IP-protokollan taso OSI-mallissa (Desmeules 2007, 17)

4.1 Syyt IPv6-protokollaan siirtymiselle

IPv4 on ollut käytössä 1970-luvun lopusta lähtien. IPv4-protokolla on osoittanut skaalautuvuutensa ja toimivuutensa pitkän toiminta-aikansa aikana. Pääasiallinen syy vaihtaa käytössä olevaa protokollaa on yksinkertaisesti IPv4:n liian pieni osoitekenttä. 32-bittisillä osoitteilla ei ole enää vähään aikaan pystynyt täyttämään ongelmattomasti IPv4-osoitteiden tarvetta. IPv4-protokollaa suunnitellessa ei osattu ottaa huomioon Internetin räjähdysmäistä kasvua. NAT- ja CIDR-tekniikoilla on saatu IPv4:n aikakautta pidennettyä ja siirtymistä IPv6:een siirrettyä. (Douglas 2002, 600 - 601.)

Tämän opinnäytetyön kirjoitushetkellä alkaa olla jo kiire suunnitella IPv6-verkkoa, sillä uusia IPv4-osoiteavaruuksia ei ole enää pitkään jaossa. Yhdysvalloissa sijaitseva IP-ositteiden maailmanlaajuinen valvonta organisaatio

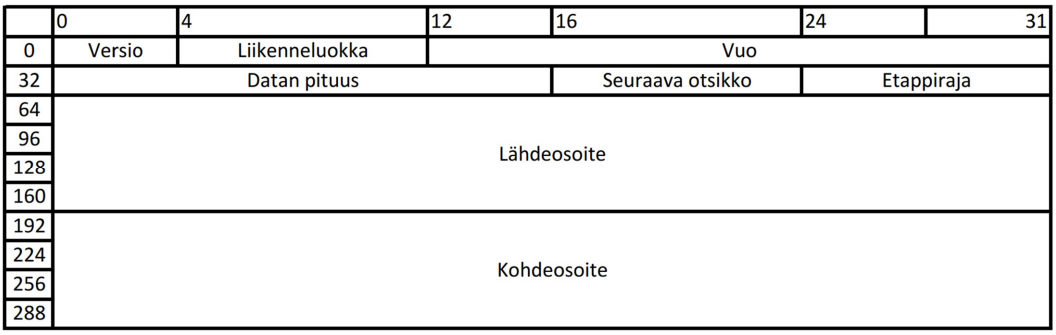
IANA (Internet Assigned Numbers Authority) on jo antanut paikallisille IP-osoitteista vastaaville organisaatioille käyttöön viimeisetkin IP-osoitteet 3.2.2011. Euroopan IP-osoiteavaruuksien jaosta operaattoreille vastaa RIPE (Réseaux IP Européens). Geoff Huston on tehnyt työkalun, joka seuraa IPv4-osoitteiden loppumista. Työkalu ennustaa, että RIPE:n kaikki osoitteet on jaettu käyttöön 2012 heinäkuussa kuvion 9 mukaisesti. Tämän jälkeen Euroopassa toimivat operaattorit eivät enää saa uusia osoiteavaruuksia, jonka jälkeen menee vielä vähän aikaa, niin operaattoreilla ei enää ole jakaa asiakkaille uusia IP-osoitteita. (Huston 2012.)



KUVIO 9. IPv4-osoitteiden loppumisen ennuste maanosittain (Huston 2012)

4.2 Kehysrakenne

Internet Protocol version 6 vähentää IP-paketin otsikon kenttien määrää. Kenttien sijainnit, nimet ja koot toisiinsa nähden oikeassa mittakaavassa on nähtävissä kuviossa 10. Uudet 128-bittiset osoitteet vievät melkein koko otsakkeen bitit.



KUVIO 10. IPv6-kehyksen perusotsikko (Douglas 2002, 604)

Ensimmäinen kenttä on versio. Kentällä on sama tarkoitus kuin IPv4:lla. Kenttä ilmoittaa, että kyseessä on IPv6-kehys, jolloin reitittimet ja muut laiteet osaavat prosessoida kehyksen oikein. Seuraava kenttä on Liikenneluokka (Traffic Class). Liikenneluokka vastaa IPv4:n TOS (Type Of Service) -kenttää. Tällä kentällä voidaan priorisoida paketteja reitittimissä. (Desmeules 2007, 46.)

Vuo-kenttä (Flow Label) on 20 bittiä pitkä. Kenttää käytetään merkkaamaan paketit, jotka kuuluvat samaan vuohon (flow). Quality of Service -palvelut voivat käyttää vuo-kenttää tunnistamaan nopeasti, mitkä paketit kuuluvat samaan vuohon, joille on haluttu taata tietty palveluntaso. Datan pituus (Payload length) -kentällä on sama tarkoitus kuin IPv4-otsakkeessa. Datan pituus -kenttä kertoo IP-pakettiin kuuluvan datan pituuden. Etappiraja (Hop limit) -kenttä vastaa IPv4:n TTL-kenttää eli kentän arvosta vähentää jokainen matkalla oleva reititin yhden. Kentän saavuttaessa arvon nolla paketti hylätään. Kenttää käytetään reitityssilmukoiden estämiseen. Lähde- ja kohdeosoitteilla on sama tarkoitus kuin IPv4-otsakkeessa, mutta kentän pituus on 128 bittiä eli IPv6-osoitteen pituinen. (Desmeules 2007, 44 - 47)

IPv6-paketin perusotsikko on aina vakion pituinen (40 oktettia). IPv6-otsakkeen jälkeen on mahdollista tulla laajennusotsikoita (Extension Header). IPv6:n perusotsakkeessa oleva kenttä seuraava otsikko (Next Header) kertoo perusotsakkeen jälkeen tulevan paketin headerin. Mikäli paketissa on laajennusotsake, tämä kenttä ilmoittaa siitä. Mikäli paketissa ei ole laajennusotsakkeita, tällöin seuraava otsikko -kenttä ilmoittaa paketin data-osassa olevan seuraavan tason protokollan. (Desmeules 2007, 44 - 47.)

4.3 Osoitteistus

Suurin muutos IPv6 protokollassa vanhempaan IPv4-protokollaan on osoitteen pituuden kasvaminen moninkertaiseksi. IPv4 tarjosi 32 bitin osoitteita, jolloin osoite oli järkevintä ilmoittaa desimaalimuodossa. Mikäli IPv6-osoitteen kirjoittaisi samassa muodossa, tulisi siitä niin pitkä, että sitä olisi haastava käsitellä. IPv6-osoitteen yleisin esitystapa on kaksoispisteillä eroteltu heksadesimaalimuoto. Kaksoispisteillä osoite jaetaan 16 bittiä pitkiin osiin (RFC 4291 2006, 3). Alla on esimerkkiosoite:

fe80:0000:0000:0000:0222:15ff:fe0e:a085

Osoite on suhteellisen pitkä ja vaikeahko muistettava, vaikka desimaalimuoto on muutettu heksadesimaalimuotoon. Osoitetta voidaan lyhentää jättämällä etunollat jokaisesta 16 bitin lohkosta pois (RFC 4291 2006, 3). Tällöin osoite saadaan muotoon:

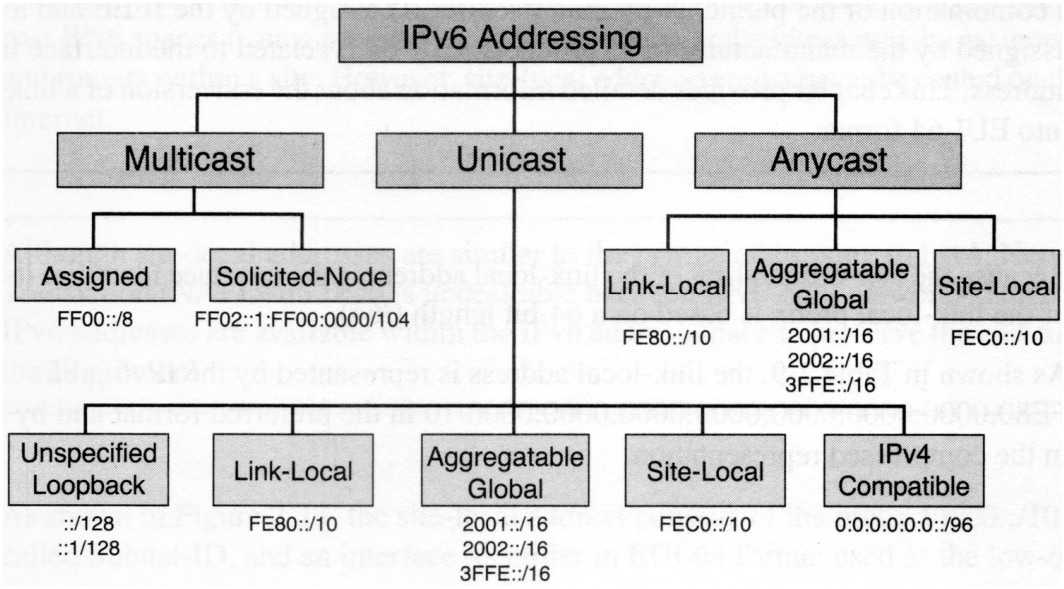
fe80:0:0:0:222:15ff:fe0e:a085

Osoite on helpompi muistaa ja kirjoittaa ilman etunollia. Osoitetta voidaan vieläkin lyhentää ottamalla osoitteesta jostakin kohtaa nollat pois ja merkkaamalla osoitteeseen kaksi kaksoispistettä peräkkäin (RFC 4291 2006, 3). Tällöin osoite voidaan kirjoittaa:

fe80::222:15ff:fe0e:a085

Huomattava asia on, että osoitteen täytyy pysyä yksiselitteisenä, vaikka sitä lyhennettäisiin. Tällöin jos osoitteessa olisi kaksi pidempää nolla-sarjaa, voidaan pelkästään toisesta paikasta lyhentää kahdella kaksoispisteellä, jolloin ohjelmistot osaavat täydentää tuplakaksoispisteen väliin niin monta nollaa, että osoitteesta tulee oikean pituinen.

IPv6-verkkoja ilmaistaessa aliverkon maskia ei ilmoiteta enää desimaalimuodossa, vaan käytetään pelkästään CIDR-muotoa. CIDR-muoto on käytössä myös IPv4 puolella. CIDR-muodossa osoitteen jälkeen ilmaistaan kauttaviivan jälkeen kuinka monta bittiä kuuluu verkko-osaan, esimerkiksi *fe80::/10*.



KUVIO 11. IPv6-osoiteavaruudet (Desmeules 2007, 61)

IPv6-osoitteet on jaettu eri avaruuksiin käyttötarkoituksen mukaan. Kuviossa 11 on jaoteltu osoitteet lähetystavan mukaan. Broadcast-liikenne on poistettu IPv6-protokollasta. Broadcast-liikenteen pääasiallinen tarkoitus oli ennen IP-osoitteen automaattiseen määritykseen ja muiden samassa verkossa olevien laitteiden etsimiseen. Tämä on korvattu multicast-liikenteellä.

Kun IPv6:sta käyttävä laite kytketään verkkoon, generoi se itselleen automaattisesti Link-Local-osoitteen. Link-Local-osoitetta käytetään samassa aliverkossa liikennöintiin sekä globaalin IPv6-osoitteen määritykseen. Link-Local-osoitetta käytetään myös, mikäli verkossa ei ole reititintä. Loopback-osoitteeksi on sovittu ::1/128. (RFC 4291 2006, 8 - 10.)

Link-Local-osoitteen automaattinen muodostus Ethernet-verkoissa tehdään yleensä MAC-osoitteesta kaavalla: fe80:0:0:0:xxxx:xxff:feyy:yyyy, jossa x tarkoittaa MAC-osoitteesta otettua valmistajan osaa ja y MAC-osoitteesta otettua verkkokortin osaa. Windows 7 -työasemissa on oletuksena päällä privacy extension -toiminto, jolloin Windows generoi Link-Local-osoitteen sattumanvaraisella menetelmällä.

Globaali Internetissä reititettävä unicast-osoiteavaruus on RFC-dokumentissa speksattu kattamaan kaikki muut paitsi yllä olevassa kuviossa olevat avaruudet (RFC 4291 2006, 5). Näistä on tällä hetkellä normaaliin IPv6-liikenteeseen

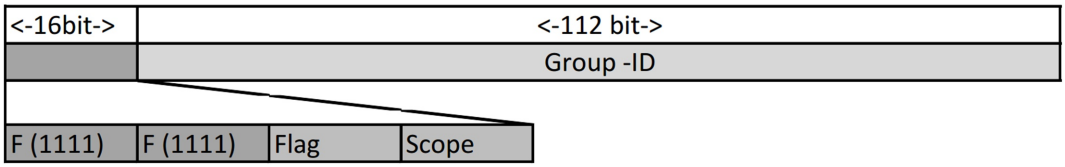
käytössä vasta 2001::/16-alue. Lisää avaruuksia tulee varmasti tarpeen mukaan käyttöön (Desmeules 2007, 67). Globaali unicast-osoite muodostuu kuvion 12 mukaisesti.

<--	128 bittiä	-->
Provider	Site	Host
2001:0708:0410:	778:	0200:CBCF:1233:4402
<--48 bittiä -->	<-16 bittiä->	<-- 64 bittiä -->

KUVIO 12. Globaalin IPv6 unicast-osoitteen rakenne (Desmeules 2007, 66)

Osoitteen alkuosan 48 bittiä tulee palveluntarjoajalta. Site-osuus on varattu osoitteen omistaman yrityksen aliverkottamista varten. Loppu 64 bittiä on varattu työasemaosaksi. Mikäli organisaatio käyttää edellä mainittua käytäntöä, on sillä tällöin käytössä 65 535 aliverkkoa, jonka pitäisi riittää lähes mihin tarkoitukseen tahansa. (Desmeules 2007, 66.)

Multicast-liikennettä käytettiin IPv4-protokollassa yleensä vain videokuvan tai äänen siirtoon yhtäaikaisesti useammalle vastaanottajalle. Toisaalta videokuva tai ääni siirretään yleensä unicast-liikenteellä, josta aiheutuu lähettäjälle paljon kuormaa, koska lähettäjä joutuu lähettämään saman lähetyksen niin monta kertaa kuin sillä on kuuntelijoita. Aika näyttää, otetaanko videokuvan ja äänen multicast-lähetykset yleisempään käyttöön IPv6-protokollan yhteydessä



KUVIO 13. Multicast-osoitteiden rakenne (Desmeules 2007, 69)

Multicast-osoitteen rakenne on esitetty kuviossa 13. Ensimmäiset 8 bittiä ovat ykkösiä. Flag eli lippukentällä voidaan ilmaista mm. onko osoite väliaikainen vai pysyvä. Scope-kenttä kertoo, kuinka laajalle multicast-paketit on tarkoitus levittää. Scope-kentän arvot on ilmaistu alla taulukossa 2. (RFC 4291 2006, 13.)

TAULUKKO 2. Multicast-osoitteen levitysalueet (RFC 4291 2006, 13)

Binääriesitys	**Heksaesitys**	**Käyttötarkoitus**
0001	1	Interface-local scope
0010	2	Link-local scope
0011	3	Subnet-local scope
0100	4	Admin-local scope
0110	5	Site-local scope
1000	8	Organisation scope
1110	E	Global scope

ARP (Address Resolution Protocol) -protokolla käyttää broadcast-liikennettä, kun halutaan selvittää samassa aliverkossa olevien laitteiden OSI-mallin toisen tason osoitteita esimerkiksi Ethernetissä MAC-osoitteita. IPv6-protokollassa alempien OSI-mallin tasojen osoitteita selvitetään multicast-paketeilla.

Osoitteiden selvittämiseksi lähetetään paketti kyseiselle laitteelle Solicited-Node Multicast –osoitteeseen. Solicited-Node Multicast –osoite muodostetaan laittamalla eteen *FF02::1:FF* ja lisäämällä perään 24 viimeistä bittiä laitteen unicast-osoitteesta. Esimerkiksi laite *FE80::222:15FF:FE0E:A085* kuuntelee Solicited-Node Multicast –osoitetta: *FF02::1:FF:0E:A085*. (Desmeules 2007, 72.)

4.4 Siirtymävaiheen tekniikat

IPv4-protokollasta ei voida siirtyä IPv6-protokollaan poistamalla ensin IPv4-protokollan ja tämän jälkeen lisäämällä IPv6-protokollan käyttöön. Verkkoliikenteessä liikennöitäessä IPv4-osoitteen omaavaan laitteeseen täytyy paketin tulla IPv4-osoitteesta, koska laite ei ymmärrä IPv6-protokollan toimintaa. IPv4-protokollan alasajoon menee arviolta kymmeniä vuosia, joten siirtymävaiheentekniikoita on tarpeen selvittää.

4.4.1 Dual-stack

Ensimmäinen tapa toteuttaa siirtymävaihe on käyttää dual-stack-tekniikkaa, jossa laitteilla on käytössä sekä IPv4- että IPv6-protokolla. Dual-stack-tekniikka aiheuttaa verkon ylläpitäjille lisätyötä, koska tällöin täytyy ylläpitää kahta eri ympäristöä. Esimerkiksi palomuurisäännöt, verkkolaitteiden konfiguraatiot ja työasemien konfiguraatiot täytyy tehdä erikseen molemmille protokollille. Työtä lievittää se, että usein on olemassa valmiiksi toimiva IPv4-ympäristö, josta voidaan ottaa mallia konfiguroitaessa IPv6-ympäristöä toimimaan. Aikoinaan, kun siirryttiin IPX (Internet Packet eXchange) -protokollasta IPv4-protokollaan, käytettiin dual-stack-ympäristöä. (Desmeules 2007, 228 - 230.)

Dual-stack-ympäristö voi aiheuttaa päätelaitteille ongelmia, mikäli IPv6-protokolla on laitteen mielestä toiminnassa, mutta vastapäässä tai verkko välissä ei tue IPv6-protokollaa. Tällöin se on sovelluksesta riippuvainen, kuinka hyvin sovellus osaa vaihtaa IPv4-protokollaan. Jos käytetään nimipalvelinta ja DNS-nimiä palveluiden saavuttamiseksi, tällöin on helppoa jättää nimipalvelusta IPv6-tietue pois, jolloin kyseiselle nimelle on vain IPv4-osoite käytössä. Mikäli jokin palvelu ei toimi, on dual-stack-ympäristössä huomattavasti enemmän vikatilannemahdollisuuksia kuin pelkällä IPv4-protokollaan perustuvalla verkolla. (Desmeules 2007, 230 - 233.)

4.4.2 Tunnelointi

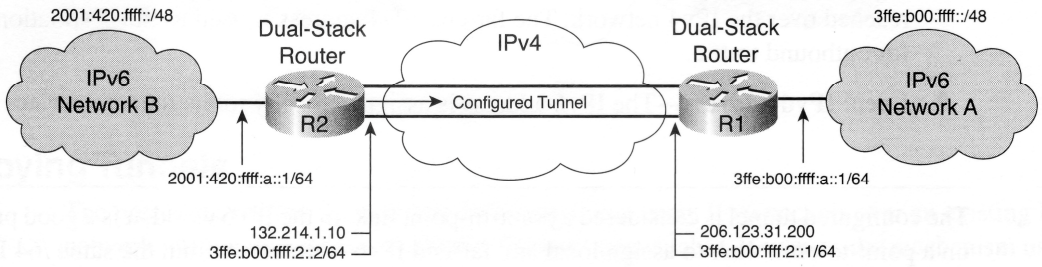
Tunneloinnissa IPv6-paketti kuljetetaan IPv4-paketin sisällä. Tunnelointi voidaan tehdä joko päätelaiteesta päätelaitteeseen, päätelaitteesta tunnelointi-palvelimeen/reitittimeen tai reitittimestä reitittimeen/tunnelointipalvelimeen. Tunneloinnilla voidaan saavuttaa esimerkiksi kahden toimipisteen välinen IPv6-yhteys käyttäen olemassa olevaa toimivaa IPv4-verkkoa tai IPv6-yhteys Internetiin, vaikka palveluntarjoaja ei tukisi IPv6-protokollaa. (Desmeules 2007, 234 -238.)

Mikäli tunnelointia halutaan käyttää, täytyy tällöin tunnelointilaitteessa (yleensä reititin tai suoraan päätelaite) olla käytössä molemmat protokollat, eli dual-stack-ympäristö. Tunnelointi aiheuttaa lisää vikaantuvia komponentteja, joten

tunnelointia ei ole suositeltavaa käyttää, mikäli se ei ole pakollista. Käyttötarkoituksesta riippuen on suositeltavaa käyttää erilaisia tunnelointimenetelmiä. Yleisimmät IPv6-tunnelointimenetelmät on esitetty taulukossa 3.

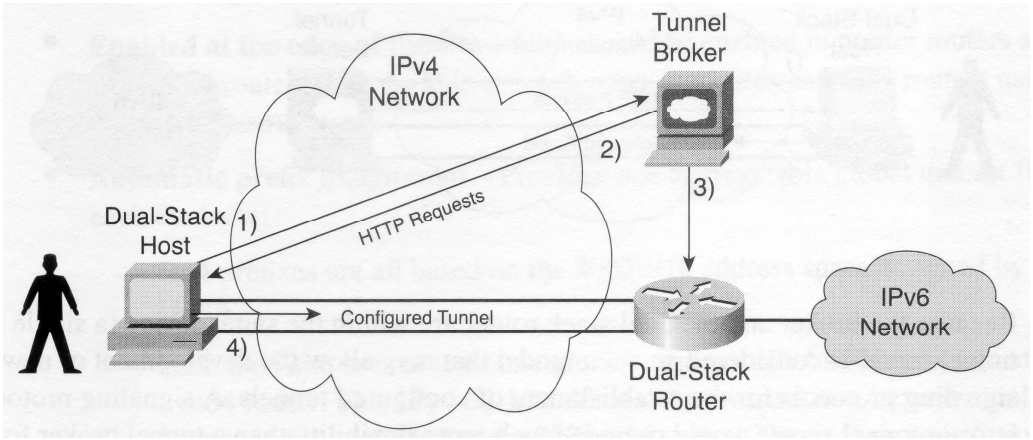
TAULUKKO 3. Yleisimmät IPv6-tunnelointimenetelmät (Desmeules 2007, 238)

Käsin tehty staattinen tunneli
Tunnel Broker
6to4
ISATAP (Intrasite Automatic Tunnel Addressing Protocol)
Teredo
IPv6 GRE tunnel



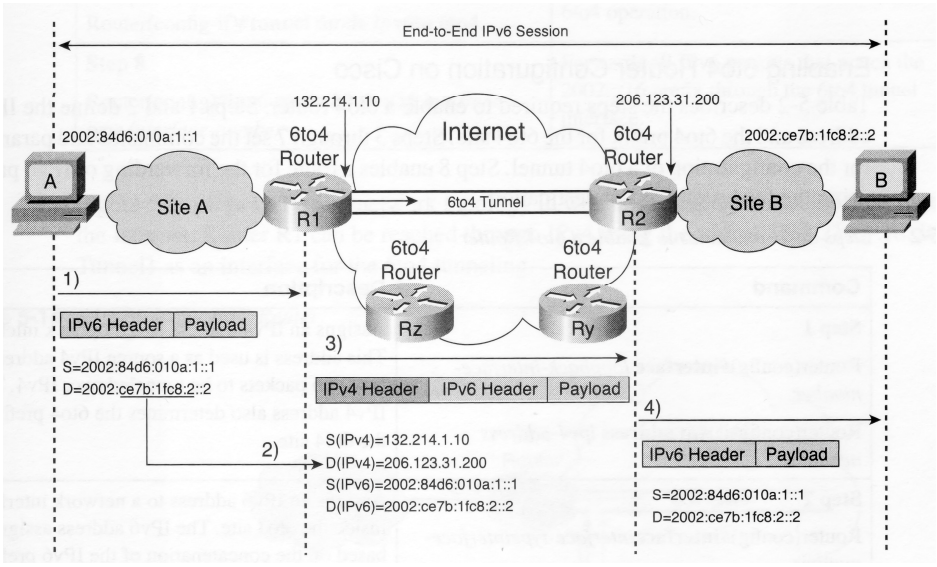
KUVIO 14. Käsin tehty staattinen tunneli (Desmeules 2007, 240)

Käsin tehdyssä staattisessa tunnelissa (kuvio 14) määritellään tunneli paikasta A paikkaan B. Tällöin IPv6-protokollaa käyttävä yhteys saadaan menemään IPv4-verkon läpi. Staattisella tunnelilla on mahdotonta toteuttaa loppukäyttäjän liittyminen verkkoon. Staattinen tunneli tehdään aina vain kahden reitittimen välille ja reitittimien täytyy tukea samaa tunnelointiprotokollaa. Mikäli useampi toimipiste halutaan liittää IPv4-verkon yli yhdeksi IPv6-verkoksi staattisilla tunneleilla, täytyy jokaisen reitittimen väli konfiguroida ja ylläpitää erikseen. Staattinen tunneli sopii siis parhaiten muutaman toimipisteen IPv6-verkkojen yhdistämiseen IPv4-verkon ylitse. (Desmeules 2007, 239 - 240.)



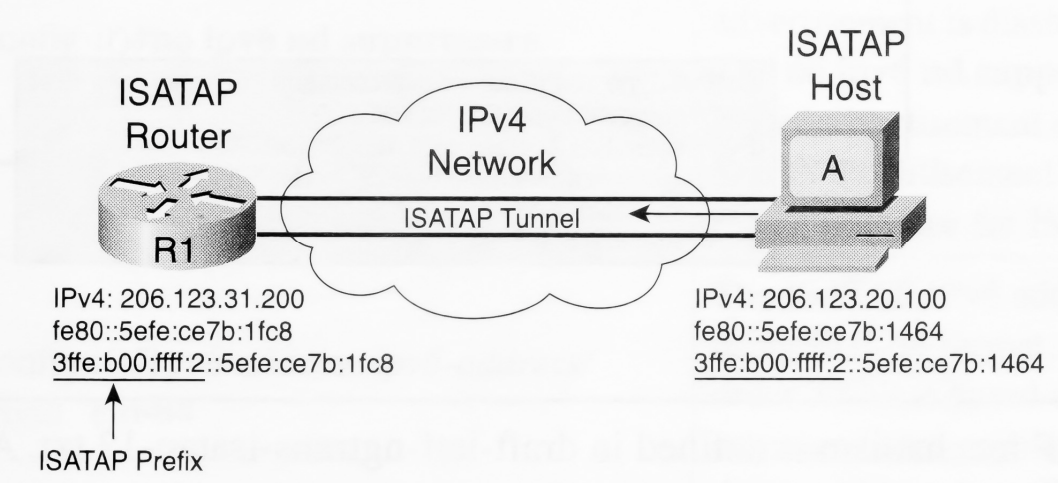
KUVIO 15. Tunnel Broker -tunneloinnin toimintaperiaate (Desmeules 2007, 243).

Tunnel Broker -tunnelointimenetelmässä tunneloidaan kuvion 15 mukaisesti useimmin loppukäyttäjä IPv6-verkkoon IPv4-verkon yli. Tunnel Broker tarvitsee neuvottelupalvelimen ja dual-stack reitittimen, jota neuvottelupalvelimella on oikeudet konfiguroida. Tunnel Broker -neuvottelupalvelimeen otetaan IPv4-osoitteella yhteys (yleisimmin käyttäen http-protokollaa) ja neuvottelupalvelin tekee reitittimeen ja loppukäyttäjän työasemaan tarvittavat määritykset tunnelin muodostamiseksi. (Desmeules 2007, 243 - 244.)



KUVIO 16. 6to4-tunneloinnin toimintaperiaate (Desmeules 2007, 247)

6to4-tunnelointi on dynaaminen kuvion 16 mukaisesti. 6to4 IPv6-osoitteen verkko-osa muodostetaan julkisesta unicast IPv4-osoitteesta, joka muutetaan heksadesimaalimuotoon ja eteen lisätään 2002. Esimerkiksi 206.123.31.200 muutettuna 6to4-osoitteeksi: 2002:ce7b:1fc8::/48. Tällöin, kun paketti lähetetään 6to4-osoitteeseen reititin tietää osoitteesta, että nyt halutaan tunneloida kyseinen paketti IPv4-verkon lävitse. IPv4-osoite, johon paketti lähetetään, pystytään päättelemään 6to4-osoitteesta. Tällöin reitittimeen tarvitsee tietää vain IPv4-protokollan reitit kohdepisteeseen. 6to4-tunnelointi ei toimi, mikäli käytetään NAT-tekniikkaa. Mikäli 6to4-tekniikalla halutaan päästä julkiseen IPv6-Internetiin, täytyy reitittimeen konfiguroida oletusreitiksi, jonkun 6to4-relay:n osoite. (Desmeules 2007, 245 - 253.)



KUVIO 17. ISATAP-tunneloinnin toimintaperiaate (Desmeules 2007, 257)

ISATAP (Intrasite Automatic Tunnel Addressing Protocol) –tunneloinnin IPv6-osoite muodostetaan ISATAP-etuliitteestä (3ffe:b00:ffff:2) ja laitteen Link-Local-osoitteen työasemaosasta kuvion 17 mukaisesti. ISATAP-tunnelointia käyttävän päätelaitteen tarvitsee tietää lista ISATAP-reitittimien IPv4-osoitteista. Reitittimien osoitteita voidaan jakaa joko käsin, DNS-palvelulla tai DHCP-palvelulla (RFC5214 2008, 6 - 7). ISATAP-tunneli muodostetaan päätelaitteen ja reitittimen välillä automaattisesti, kunhan se on konfiguroitu toimintaan reitittimen ja päätelaitteen päässä. (Desmeules 2007, 256 - 259.)

Teredo-tunneloinnilla otetaan yhteyttä Teredo-palvelimeen ja palvelin on yhteydessä IPv6-verkkoon, yleensä julkiseen Internetiin. Teredo-tunnelointi käyttää UDP-protokollaa tunnelointiin. IPv6-paketti on kapseloitu IPv4-protokollaa käyttävän UDP-paketin Payload eli data-osioon. Tämän avulla Teredo tukee hyvin NAT-laitteen takana olevia päätelaitteita. Teredo-tunnelointi lisää viivettä ja vaatii palvelimelta paljon kapasiteettia, joten sitä ei tulisi käyttää, mikäli on mahdollista IPv6-yhteys muuta tapaa käyttäen. (RFC4380 2006, 7 - 8)

Mikäli ympäristöön, jossa käytetään VPN (Virtual Private Network) –tunnelointia takaamaan suojatun yhteyden päätelaitteen ja yrityksen sisäverkon välille tai usean toimipisteen yhdistämiseen, voidaan yleensä samassa VPN-tunnelissa tunneloida myös IPv6-protokollaa, vaikka paketit kulkisivatkin julkisen IPv4-verkon lävitse. Esimerkiksi Anyconnect-VPN-tunnelointi tukee IPv6-protokollaa IPv4-verkon yli (Cisco 2010). Toinen esimerkki on GRE-tunnelointi (Desmeules 2007, 254 - 255).

4.4.3 NAT64

NAT64-tekniikalla pystyy yhdistämään IPv4- ja IPv6-verkkoja keskenään. NAT64 muuntaa IPv6-osoitteita IPv4-osoitteiksi. Useimmiten NAT64 on toiminnassa reitittimessä, johon on kytketty sekä IPv4-, että IPv6-verkkoja. NAT64-tekniikasta on olemassa kaksi vaihtoehtoa: tilaton ja tilallinen.

TAULUKKO 4. Tilallisen ja tilattoman NAT64 vertailu (Cisco 2011)

Tilaton NAT64	Tilallinen NAT64
Vain 1:1 osoitteenmuunnos	Dynaaminen 1:n osoitteenmuunnos
Vie yhtä muunnosta kohden yhden IPv4-osoitteen	Säästää IPv4-osoitteita
Yhteyksien tilaa ei pidetä muistissa, vie vähemmän kapasiteettia	Jokaisen yhteyden tila tiedossa
Vaatii IPv4-osoitteeksi kääntämiseen	Osoitteet voivat vaihdella

soveltuvan IPv6-osoitteen	dynaamisuuden takia
Päätelaitteiden IPv4-osoitteet täytyy joko laittaa käsin tai DHCPv6 palvelimelta	IPv6-osoitteiden määritystavalla ei ole merkitystä

Tilallinen NAT64 muuntaa useita IPv6-osoitteita yhdeksi IPv4-osoitteeksi, kun taas tilaton muuntaa kiinteästi yhden IPv4-osoitteen yhdeksi IPv6-osoitteeksi. Mikäli NAT64-muunnoksen taakse halutaan vähän laitteita, on tällöin tilaton toimintavarmempi, mutta laitteita ollessa paljon on tilaton työläämpi vaihtoehto. Tilallista NAT64 voidaan tilatonta helpommin ylläpitää, mikäli laitteita on paljon. NAT64-osoitteenmuunnosta voidaan käyttää esimerkiksi jos työasemaverkossa olisi pelkästään IPv6-protokolla käytössä ja sieltä haluttaisiin tulostaa tulostimella, joka ymmärtää vain IPv4-protokollaa. (Cisco 2011.)

5 PHKK:N NYKYISTEN VERKKOLAITTEIDEN IPV6 TUKI

RIPE:n (Réseaux IP Européens) IPv6 työryhmä on tehnyt listauksen ICT-laitteiden ominaisuuksista, jotka tulisi IPv6-ympäristössä toimia. Tämän listan perusteella tarkastellaan, mitä ominaisuuksia PHKK:n runkoverkossa olevat laitteet tukevat. Dokumentti Requirements For IPv6 in ICT Equipment on julkaistu 20.10.2010 ja dokumentti löytyy RIPE:n verkkosivuilta osoitteesta: http://www.ripe.net/ripe/docs/ripe-501.

5.1 Palomuurit

RIPE:n IPv6-työryhmän dokumentissa Requirements For IPv6 in ICT Equipment on määritelty keskeisiä ominaisuuksia verkon tietoturvalaitteille, kuten palomuureille. Nämä keskeiset ominaisuudet on listattu taulukossa 5. Taulukossa lukee ensin ominaisuus, sitten missä RFC-dokumentissa ominaisuus on kuvattu ja lopussa sulkeissa, mitä verkon laitteita kyseinen ominaisuus koskee. FW (Firewall) tarkoittaa palomuurilaitteita, IPS (Intrusion prevention system) tarkoittaa verkon paketeista haitallista liikennettä etsiviä laitteita ja APFW tarkoittaa ohjelmallisia palomuureja. Tässä opinnäytetyössä ei oteta kantaa ohjelmallisiin palomuureihin.

TAULUKKO 5. RIPE:n suosittelemat palomuurien vähimmäis IPv6-ominaisuudet (Žorž & Steffann 2010)

IPv6 Basic specification [RFC2460] (FW, IPS, APFW)
IPv6 Addressing Architecture basic [RFC4291] (FW, IPS, APFW)
Default Address Selection [RFC3484] (FW, IPS, APFW)
ICMPv6 [RFC4443] (FW, IPS, APFW)
SLAAC [RFC4862] (FW, IPS)
Router-Alert option [RFC2711] (FW, IPS)
Path MTU Discovery [RFC1981] (FW, IPS, APWF)
Neighbor Discovery [RFC4861] (FW, IPS, APFW)
If the request is for the BGP4 protocol, the equipment must comply with RFC4271, RFC1772, RFC4760 and RFC2545 (FW, IPS, APFW)

If the request is for a dynamic internal guidance protocol (IGP), then the required RIPng [RFC2080], OSPF-v3 [RFC5340] or IS-IS [RFC5308]. The contracting authority shall specify the required protocol. (FW, IPS, APFW)
If the requested OSPF-v3, the device must support "Authentication/Confidentiality for OSPFv3" [RFC4552] (FW, IPS, APFW)
Support for QoS [RFC2474, RFC3140] (FW APFW)
Basic Transition Mechanisms for IPv6 Hosts and Routers [RFC4213] (FW)
Using IPsec to Secure IPv6-in-IPv4 Tunnels [RFC4891] (FW)

Palomuureina PHKK:ssa käytetään Ciscon ASA -palomuurien eri versioita sekä sisäisenä palomuurina Cisco FWSM -moduulia reitittävissä kytkimissä. PHKK:n palomuureissa on tällä hetkellä käytössä staattiset reitit, joten laitteiden ei tarvitse tukea reititysprotokollia. IPv6-osoitteiden automaattinen generointi reitittimen mainostamaan verkkoon työaseman MAC-osoitteesta, SLAAC (Stateless address autoconfiguration), ei tarvitse olla tuettuna, koska tarkoituksena on käyttää DHCPv6-palvelinta IPv6-osoitteiden määritykseen. Loppujen lopuksi Dual Stack –tuki, access-listojen tekeminen IPv6-osoitteilla ja staattisten reittien tekeminen IPv6-osoitteilla ovat riittävät vaatimukset verkon reunalla oleviin Cisco ASA palomuureihin, jotka täyttyvät käytössä olevassa vanhimmassakin ohjelmistoversiossa. Sisäinen palomuuri, joka on FWSM-moduuli runkoreitittimissä, tukee IPv6-protokollaa nykyisessä versiossaan.

5.2 Reitittimet

RIPE:n IPv6-työryhmän dokumentissa Requirements For IPv6 in ICT Equipment on käsitelty myös reitittimien keskeisiä vaatimuksia. Lista on kattava, ja pienemmissä ympäristöissä ei tarvitse lähellekään kaikkia listan ominaisuuksia. Ominaisuudet on listattu taulukossa 6.

TAULUKKO 6. RIPE:n suosittelemat reitittimien vähimmäis IPv6-ominaisuudet (Žorž & Steffann 2010)

IPv6 Basic specification [RFC2460]
IPv6 Addressing Architecture basic [RFC4291]

Default Address Selection [RFC3484]
ICMPv6 [RFC4443]
SLAAC [RFC4862]
MLDv2 snooping [RFC4541]
Router-Alert option [RFC2711]
Path MTU Discovery [RFC1981]
Neighbor Discovery [RFC4861]
Classless Inter-domain routing [RFC4632]
If dynamic internal guidance protocol (IGP) is requested, then RIPng [RFC2080], OSPF-v3 [RFC5340] or IS-IS [RFC5308] must be supported. The contracting authority shall specify the required protocol.
If OSPF-v3 is requested, the equipment must comply with "Authentication/Confidentiality for OSPF-v3" [RFC4552]
If BGP4 protocol is requested, the equipment must comply with RFC4271, RFC1772, RFC4760, RFC1997, RFC3392 and RFC2545
Support for QoS [RFC2474, RFC3140]
Basic Transition Mechanisms for IPv6 Hosts and Routers [RFC4213]
Using IPsec to Secure IPv6-in-IPv4 tunnels [RFC4891]
Generic Packet Tunneling and IPv6 [RFC2473]
If 6PE is requested, the equipment must comply with "Connecting IPv6 Islands over IPv4 MPLS Using IPv6 Provider Edge Routers (6PE)” [RFC4798]
Multicast Listener Discovery version 2 [RFC3810]
If mobile IPv6 is requested, the equipment must comply with MIPv6 [RFC3775, RFC5555] and "Mobile IPv6 Operation With IKEv2 and the Revised IPsec Architecture" [RFC4877]
If MPLS functionality (for example, BGP-free core, MPLS TE, MPLS FRR) is requested, the PE-routers and route reflectors must support "Connecting IPv6 Islands over IPv4 MPLS Using IPv6 Provider Edge Routers (6PE)" [RFC 4798]
If layer-3 VPN functionality is requested, the PE-routers and route reflectors must support "BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN" [RFC 4659]
If MPLS Traffic Engineering is used in combination with IS-IS routing protocol, the equipment must support "M-ISIS: Multi Topology (MT) Routing in

Intermediate System to Intermediate Systems (IS-ISs)" [RFC 5120]

PHKK:lla on käytössä reitittiminä OSI-mallin kolmannella tasolla toimivat kytkimet. Kytkinten malli on Cisco Catalyst 6500. Näissä PHKK:n runkoverkon pääkytkimissä on kaikki reititys, minkä takia työssä nimitetään niitä jäljempänä reitittimiksi. Reitittimien ohjelmisto on Ciscon oma IOS. Reitittimienkään ei tarvitse tukea tilatonta IPv6-osoitteiden automaattista generointia, eli SLAAC:a, mutta sen sijaan DHCPv6 relay -toiminto pitää olla tuettuna, koska halutaan käyttää vain yhtä DHCPv6-palvelinta, joka jakaa useaan aliverkkoon IPv6-osoitteita. Tämä ominaisuus oli RIPE:n optionalisten suosituksien listalla. Lisäksi, mikäli DHCPv6-palvelinta halutaan käyttää, täytyy reitittimiin pystyä asettamaan reititinmainostuksiin *managed config* -lippu, joka viestittää päätelaitteille, että IPv6-osoitteet tulisi hakea DHCPv6-palvelimelta oletusreitin tullessa kuitenkin reititinmainostuksesta. PHKK:n verkon rakenteesta johtuen laitteessa on useita eri virtuaalisia reititystauluja, eli VRF:iä, koska PHKK:lla on erilaisia verkkoja, joiden keskinäistä liikennöintiä halutaan rajoittaa. VRF:ien tuki tulisi olla myös IPv6 osoitteilla.

Vanhassa ohjelmistoversiossa oli vain yksinkertaisia IPv6-ominaisuuksia, eli muun muassa IPv6-osoitteiden laittaminen liitynnöille, staattisten reittien teko globaaliin reititystauluun ja reititinmainostusten *managed config* -lipun asetus. Koko PHKK:n verkon looginen rakenne perustuu virtuaalisten reititystaulujen (VRF) käyttöön, jonka takia ohjelmisto jouduttiin päivittämään versioon, johon on lisätty kaikki aiemmin mainitut ominaisuudet. Uudempaan ohjelmistoon on tullut uutena ominaisuuksina muun muassa seuraavat kriittiset ominaisuudet: VRF:ien toiminta IPv6-protokollalla, Ciscon reitittimien automaattisen kahdennus-protokollan eli HSRP:n (Hot Standby Router Protocol) tuki IPv6-osoitteilla ja DHCP relay -toiminto IPv6-protokollalla.

5.3 OSI-mallin toisen tason kytkimet

RIPE:n IPv6-työryhmä on määritellyt myös OSI-mallin toisen tason kytkimille vaatimuksia, jotta niitä voidaan nimittää IPv6-yhteensopiviksi. OSI-mallin toisen tason kytkimet eivät varsinaisesti ota kantaa siihen, mitä protokollaa OSI-mallin

tasolla kolme kuljetetaan, mutta silti kytkimissä on hyvä olla ominaisuuksia, joilla parannetaan tietoturvaa. Requirements For IPv6 in ICT Equipment -dokumentin OSI-mallin toisen tason kytkinten vaatimusten lista löytyy taulukosta 7.

TAULUKKO 7. RIPE:n suosittelemat L2-kytkinten vähimmäis IPv6-ominaisuudet (Žorž & Steffann 2010)

MLDv2 snooping [RFC4541]
DHCPv6 snooping [RFC3315], DHCPv6 messages must be blocked between subscribers and the network so that false DHCPv6 servers cannot distribute addresses.
Router Advertisement (RA) filtering [RFC4862, RFC5006], RA filtering must be used in the network to block unauthorized RA messages.
Dynamic "IPv6 neighbor solicitation/advertisement" inspection [RFC4862], There must be an IPv6 neighbor solicitation/advertisement inspection, as in IPv4 "Dynamic ARP Inspection". The table with MAC-address and link-local and other assigned IPv6-addresses must be dynamically created by SLAAC or DHCPv6 messages.
Neighbor Unreachability Detection [NUD, RFC4861] filtering, There must be a NUD filtering function to ensure that false NUD messages cannot be sent.
Duplicate Address Detection [DAD, RFC4429] snooping and filtering, Only authorized addresses may be allowed as source IPv6 addresses in DAD messages from each port

OSI-mallin toisen tason vaatimukset liittyvät kaikki tietoturvan parantamiseen MLDv2 snoopingia lukuun ottamatta. MLDv2 snooping on tuettu Cisco Catalyst 2960-S sarjan kytkimissä, muttei vanhemmissa 2960G-malleissa. MLDv2 snooping ei ole tuettu PHKK:n käytössä olevissa HP:n Pro Curve -kytkimissä, ei edes uusimmissa 2810 malleissa. Tietoturvaominaisuuksien tukeminen on kaikissa kytkimissä tällä hetkellä heikkoa, kuten myös Ciscon kytkimissä. Taulukossa 7 mainituista tietoturvaa lisäävistä ominaisuuksista tuettuna on ainoastaan Duplicate Address Detection.

5.4 Ciscon valmistamat langattomat verkot

RIPE:n dokumentissa Requirements For IPv6 in ICT Equipment ei ole mainintaa langattomien verkkojen suosituksista. Ciscon langaton verkko tunneloi runkoverkosta yhteydet radiotien ylitse kannettavalle päätelaitteelle, joten sillä ei pitäisi olla merkitystä, mitä protokollaa langattomasti kuljetetaan. Langattomat päätelaitteet eivät voi suoraan keskustella keskenään, vaan yhteys kulkee vähintään runkokytkimen tai runkokytkimien ja reitittimen kautta, jolloin kytkinten tietoturva koskettaa myös langatonta järjestelmää.

Langattomien päätelaitteiden liittyessä langattoman järjestelmän ohjain autentikoi käyttäjän 802.1x-protokollalla. Langattoman järjestelmän ohjain ei tue nykyisessä ohjelmistoversiossa IPv6-pakettien avulla tehtävää autentikoitumista, jolloin päätelaitteilla tulee olla Dual Stack –tuki autentikoinnin tapahtuessa IPv4-protokollalla muun liikenteen käyttäessä IPv6-protokollaa.

5.5 Linux-palvelut

Linux-palvelut tukevat hyvin IPv6:sta. Linuxin ydin eli kernel tukee IPv6:sta jollain tasolla 2.2 versiosta lähtien (Bieringer 2009). Versio 2.4.x tukee IPv6:sta, mutta sille ei enää kehitetä uusia ominaisuuksia, joten suositeltavaa on käyttää 2.6.x versiota tai uudempaa IPv6 verkoissa (Bieringer 2009). Nykyisessä konsernin Linuxilla toimivassa DNS- ja DHCP-palvelimessa on käytössä riittävän uusi versio.

DHCP-palveluna käytetään ISC:n (Internet Systems Consortium) DHCP-palveluun. ISC DHCP -palveluun on tullut IPv6-tuki versiosta 4.x alkaen (Bieringer 2009). ISC DHCP -palvelinta ei voida yhdellä prosessilla ajaa siten, että palvelin jakaisi sekä IPv4- että IPv6-osoitteita, minkä takia täytyy ajaa kahta eri prosessia, jos molempien halutaan olevan käytössä (Bieringer 2009). Nykyinen konsernin DHCP-palvelu vaatii päivittämistä uudempaan versioon, jotta palvelu tukisi IPv6-protokollaa.

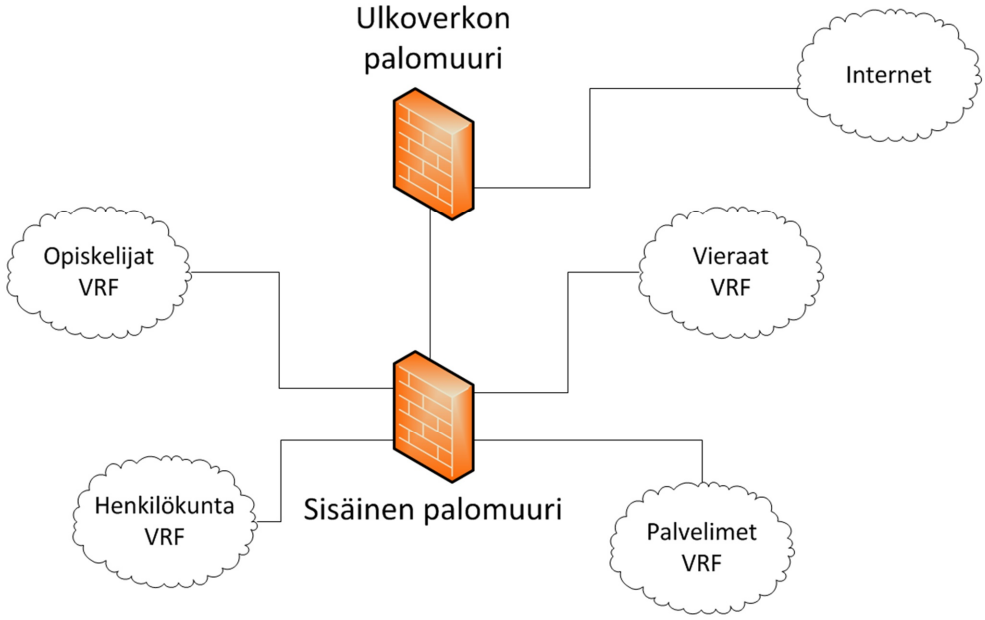
DNS-palveluna käytetään ISC:n BIND (Berkeley Internet Name Domain) -palvelua. BIND sisältää IPv6-tuen alkaen versiosta 9.x, mutta suositellaan käytettäväksi vähintään 9.1.3-versiota, jossa on paikattu tietoturva-aukkoja

(Bieringer 2009). DNS-palvelua ei tarvitse välttämättä päivittää PHKK:lla, koska käytössä on riittävän uusi versio.

6 TARVITTAVAT MUUTOKSET PHKK:N VERKKOON

6.1 Nykyisen verkon kuvaus

PHKK:n nykyinen verkko toimii IPv4-protokollalla. Erilaisille käyttäjille on tehty erilaisia verkkoja, jotka on liitetty virtuaalisiin reititystauluihin eli VRF:iin. Mikäli virtuaalisesta reititystaulusta halutaan liikennöidä jonkun muun virtuaalisen reititystaulun työasemalle tai palvelimelle, menee yhteys sisäisen palomuurin kautta, jossa yhteyksiä voidaan rajoittaa ja kontrolloida. Lisäksi ulkoverkon yhteyksiä varten on olemassa oma palomuurinsa, jossa tehdään verkosta riippuen myös NAT-osoitteenmuunnos. Kuviossa 18 on esitetty topologia yksinkertaistettuna.



KUVIO 18. PHKK:n runkoverkon topologia

Jokainen VRF voi sisältää useita verkkoja, jotka on jaoteltu muun muassa toimipisteen mukaan. VRF:ien avulla on helppo toteuttaa monimutkaisiakin palomuurisääntöjä muutosten pysyessä yksinkertaisina. Sisäinen palomuuri on FWSM-palomuurimoduuli runkoreitittimissä. Ulkoinen palomuuri on Ciscon ASA 5500 -sarjan palomuuri.

6.2 Toteutustavan valinta

PHKK:n verkko toimii valmiiksi hyvin ja tehokkaasti, joten verkkotopologiaan ei tehdä muutoksia. PHKK:n verkko menee joko suorilla kaapeleilla toimipisteestä toiseen tai kaukaisimmat toimipisteet menevät operaattorin MPLS-verkossa, minkä takia tunnelointiprotokollia ei kannata ottaa käyttöön, vaan niiden käyttö estetään palomuurissa. Dual-stack-tekniikka tulee olemaan toteutustapa sen kohtuullisen yksinkertaisen toteutustavan vuoksi. Tällöin vanha toimiva IPv4-verkko jää toimintaan. IPv6-protokollan puolelle tullaan tulevaisuudessa ottamaan palveluja käyttöön, jolloin vikatilanteita tullaan tarkkailemaan. Tunneleiden tai NAT64-osoitteenmuunnosta tullaan harkitsemaan uudelleen siinä vaiheessa, kun suurin osa verkosta käyttää IPv6-protokollaa.

Dual-stack-toteutuksen työläin osa tulee olemaan palomuurisääntöjen ylläpito, koska mikäli molemmat protokollat ovat käytössä, tällöin on myös palomuuri säännöt kirjoitettava identtisinä molemmilla protokollilla. Reitittimien ohjelmisto joudutaan päivittämään, mutta muutoin verkko on nykyisillä laitteilla valmis Dual-stack-ympäristön tekemiseen.

6.3 Reititin

Reitittimeen R1 määritettiin ensin seuraavat perus IPv6-määritykset. Ensin asetettiin globaalille konfiguraatio tasolle komento: *ipv6 unicast-routing*. Tämän jälkeen määritettiin liitynnälle perusasetukset:

```
interface vlan xx8
        ipv6 nd prefix default no-advertise
        ipv6 nd managed-config-flag
        ipv6 address 2001:708:410:xx8::y/64
```

Komennolla *ipv6 address* annettiin liitynnälle IPv6-osoite. Komennolla *ipv6 nd managed-config-flag* määritettiin managed-config-lippu päälle, joka viestittää työasemille, että käytössä on erillinen DHCP-palvelin, jolloin kysellään IPv6-osoite, DNS-palvelin ja muut määrittelyt lukuun ottamatta oletusreittiä, joka tulee suoraan reitittimeltä. Komennolla *ipv6 nd prefix default no-advertise* reititin ei mainosta mitään muuta kuin oletusreittiä. Näillä konfiguratioilla pystyttiin testaamaan DHCP-palvelun toiminta. Seuraavana vuorossa oli reitittimien

päivitys. Operaattori päivitti reitittimet, koska PHKK:lla on operaattorin kanssa osaan runkoverkon laitteisiin ylläpitosopimus. Kun reitittimet saatiin päivitettyä, päästiin reititin konfiguroimaan Dual-stack-ympäristöä varten. Aluksi luotiin testikäyttöä varten kaksi VRF:ä.

```
mls ipv6 vrf
vrf definition <ipv6 ws vrf >
        rd zzzzz:zz
        route-target export zzzzz:zz
        route-target import zzzzz:zz
        !
        address-family ipv4
        exit-address-family
        !
        address-family ipv6
        exit-address-family
       !
vrf definition <ipv6 server vrf>
        rd zzzzz:zz
        route-target export zzzzz:zz
        route-target import zzzzz:zz
        !
        address-family ipv4
        exit-address-family
        !
        address-family ipv6
        exit-address-family
```

Komennolla *mls ipv6 vrf* otettiin globaalisti VRF:issä käyttöön IPv6-protokolla. Tämän jälkeen VRF:t luotiin komennoilla *vrf definition <vrf name>*. VRF:ille määritettiin saman lailla kuin muillekin IPv4-VRF:ille *rd* ja *route-targetit*. VRF:ien alla täytyy kertoa, mitä IP-protokollia kyseisessä VRF:ssä käytetään. Testikäytössä oleviin virtuaalisiin reititystauluihin otettiin Dual Stack ratkaisun mukaisesti sekä IPv4 -, että IPv6-protokollat. VRF:ien teon jälkeen määritettiin reitittimien ja palomuurimoduulien väliset linkkiverkot. Nämä tehtiin komennoilla:

```
interface Vlan xx
        vrf forwarding <ipv6 ws vrf >
        ip address a.a.a.a b.b.b.b
        ipv6 address 2001:708:410:xx::y/64
        standby version 2
        standby 1 ip a.a.a.d
        standby 1 priority 105
        standby 1 preempt
```

```
        standby 1 authentication md5 key-string ****
        standby 2 ipv6 2001:708:410:xx::z/64
        standby 2 priority 105
        standby 2 preempt
        standby 2 authentication md5 key-string ****

!
interface Vlan xx
        vrf forwarding <ipv6 server vrf>
        ip address a.a.a.a b.b.b.b
        ipv6 address 2001:708:410:xx::y/64
        standby version 2
        standby 1 ip a.a.a.d
        standby 1 priority 105
        standby 1 preempt
        standby 1 authentication md5 key-string ****
        standby 2 ipv6 2001:708:410:xx::z/64
        standby 2 priority 105
        standby 2 preempt
        standby 2 authentication md5 key-string ****
```

Komennoista on sensuroitu vlanien numerot, VRF:ien nimet, kaikki IP-osoitteet ja HSRP –protokollan salausavain. Komennolla *vfr forwarding <vrf name>* kerrotaan, mitä virtuaalista reititystaulua kyseisessä verkossa tulisi käyttää. Tämä komento on muuttunut IPv6-tukevissa VRF:issä komennon ollessa aikaisemmin *ip vfr forwarding.* Seuraavaksi määritettiin liitynnöille IPv4- ja IPv6-osoitteet. Ciscon reitittimien automaattinen kahdennusprotokolla HSRP tukee versiossa kaksi IPv6:sta. HSRP:n versiossa kaksi on myös mahdollisuus salata autentikoitumis avain md5-hashilla ja se otettiin myös käyttöön komennoilla *standby <process number> authentication md5 key-string* ****, jossa **** on käytettävä salausavain. Salausavainta käytetään reitittimien keskinäiseen tunnistamiseen. HSRP-prosesseja täytyi ottaa käyttöön kaksi per vlan, koska yksi prosessi voi ajaa vain joko IPv4-, tai IPv6-protokollaa. Muut vlanien asetukset kopioitiin olemassa olevista vlaneista.

Seuraavaksi luotiin verkot, joihin testilaitteet kytketään. Verkkojen luonti on hyvin samankaltainen kuin linkkiverkkojenkin. Verkot luotiin komennoilla:

```
interface Vlan xx7
        description ipv6-testiverkko tyoasemille
        vrf forwarding <ipv6 ws vrf >
        ip address a.a.a.a b.b.b.b
```

```
        ip helper-address c.c.c.c
        standby version 2
        standby 1 ip a.a.a.d
        standby 1 priority 105
        standby 1 preempt
        standby 1 authentication md5 key-string ****
        standby 2 ipv6 2001:708:410:xx7::z/64
        standby 2 priority 105
        standby 2 preempt
        standby 2 authentication md5 key-string ****
        ipv6 address 2001:708:410:xx7::y/64
        ipv6 nd prefix default no-autoconfig
        ipv6 nd managed-config-flag
        ipv6 dhcp relay destination 2001:708:410:xxx::yy
!
interface Vlan xx8
        description ipv6-testiverkko palvelimille
        vrf forwarding <ipv6 server vrf>
        ip address a.a.a.a b.b.b.b
       standby version 2
        standby 1 ip a.a.a.d
        standby 1 priority 105
        standby 1 preempt
        standby 1 authentication md5 key-string ****
        standby 2 ipv6 2001:708:410:xx8::z/64
        standby 2 priority 105
        standby 2 preempt
        standby 2 authentication md5 key-string ****
        ipv6 address 2001:708:410:xx8::y/64
        ipv6 nd prefix default no-autoconfig
```

Erona linkkiverkkoihin on, että työasemaverkossa käytetään DHCP-palvelinta ja palvelinverkossa otettiin pois käytöstä SLAAC tilaton IPv6-osoitteiden jako. Komennolla *ipv6 nd prefix default no-autoconfig* otettiin pois käytöstä SLAAC tilaton IPv6-osoitteiden jako. Komennolla *ipv6 nd managed-config-flag* asetettiin reititinmainostuksiin M-lippu päälle, joka kertoo päätelaitteelle, että lisäasetuksia tulee kysyä DHCPv6-palvelimelta. DHCPv6-palvelin sijaitsi palvelin IPv6-verkossa, joten tällöin työasemaverkolle konfiguroitiin DHCP relay -toiminto, joka välittää DHCPv6-paketteja eri verkkoon. Tämä tehtiin komennolla: *ipv6 dhcp relay destination <IPv6 -osoite>*.

PHKK:n runkoverkossa käytetään staattisia reittejä, joten näidenkin verkkojen reititys tehtiin staattisilla reiteillä. Reitittimeen asetettiin vielä staattiset oletusreitit

työasema ja palvelin verkoista linkkiverkkojen palomuurien osoitteisiin sekä IPv4-, että IPv6-protokollilla. Nämä tehtiin komennoilla:

ip route vrf <ipv6 server vrf> 0.0.0.0 0.0.0.0 a.a.a.a
ip route vrf <ipv6 ws vrf > 0.0.0.0 0.0.0.0 a.a.a.a
ipv6 route vrf <ipv6 server vrf> ::/0 2001:708:410:xx::y
ipv6 route vrf <ipv6 ws vrf >::/0 2001:708:410:xx::y

Asetukset kopioitiin R2-reitittimeen, vaihtaen IP-osoitteet. Näiden reitittimen ja palomuurin asetusten jälkeen toiminta testattiin ja verkko toimi kuten oletettiin. Konfiguraatiot kopioitiin toiseen reitittimeen muuttaen IP-osoitteet. HSRP:n toiminta testattiin, ja sekin toimi kuten oletettiin paitsi, että katsoessa HSRP:n toimintaa *show standby brief* -komennolla näytti reititin HSRP-osoitteiksi link local -osoitteet. Jotta toinen reititin ottaa haltuunsa VRF:n reitityksen, täytyy sekä linkkiverkon että työasemaverkon lakata toimimasta ykkösreitittimessä.

6.4 Palomuuri

Ulkoverkkoon eli Internetiin ei ollut IPv6-yhteyttä opinnäytetyön teon aikana, joten ulkoverkon palomuuriin ei tehty mitään asetuksia. Sisäinen palomuuri oli näiden kahden testi VRF:n välissä, joten palomuurisäännöt tehtiin ainoastaan näiden kahden verkon välille. Sisäiseen palomuuriin määritettiin ensin liitynnät. Alla on esimerkki yhden liitynnän vaatimista komennoista, joista on sensuroitu IP-osoitteet, vlan id:t, ja security-level.:

interface Vlan xxx
security-level aa
ip address c.c.c.c d.d.d.d
ipv6 address 2001:708:410:xxx::z/yy

Molemmille uusille vlaneille tehtiin uudet liitynnät ja ulkoliitynnälle annettiin myös IPv6-osoite. Liityntöjen määritysten jälkeen tehtiin reitit IPv4- ja IPv6-protokollilla. Alla on esimerkki IPv6-reitin tekemisestä:

ipv6 route <ipv6 srv vrf> 2001:708:410:xx7::/zz
2001:708:410:yy::vvvv

Reittien tekeminen ei eroa käytettiin IPv4- tai IPv6-protokollaa, paitsi edessä oleva määritys *ip* vaihtuu *ipv6*-määritykseen. Lopuksi, jotta liikenne kulkisi,

täytyy tehdä vielä pääsylistat (access-list). Pääsylistoilla määrätään mistä on oikeus liikennöidä minnekin milläkin protokollalla. Alla on esimerkki molemmilla protokollilla tehdyistä pääsylistoista:

ipv6 access-list <id> permit ip 2001:708:410:xx8::/yy 2001:708:410:xx7::/yy
access-list <id> extended permit ip any a.a.a.a b.b.b.b

Esimerkin pääsylistoilla sallittiin IPv6 testi palvelin -verkosta liikennöinti sekä IPv4-, että IPv6-protokollalla IPv6 testi työasema -verkkoon. Tämän jälkeen tehtiin vielä sääntö toisinpäin. Pääsylistojen teon jälkeen liikenne lähti toimimaan hyvin. Todellisuudessa näin löysiä sääntöjä ei kuitenkaan tehdä, joten esto-sääntöäkin kokeiltiin. Esimerkiksi IPv6 testi työasema -verkosta kiellettiin SSH-protokolla IPv6 testi palvelin -verkkoon molemmilla protokollilla:

ipv6 access-list <id> deny tcp 2001:708:410:xx7::/yy 2001:708:410:xx8::/yy eq ssh
access-list <id> extended deny tcp a.a.a.a b.b.b.b c.c.c.c b.b.b.b eq ssh

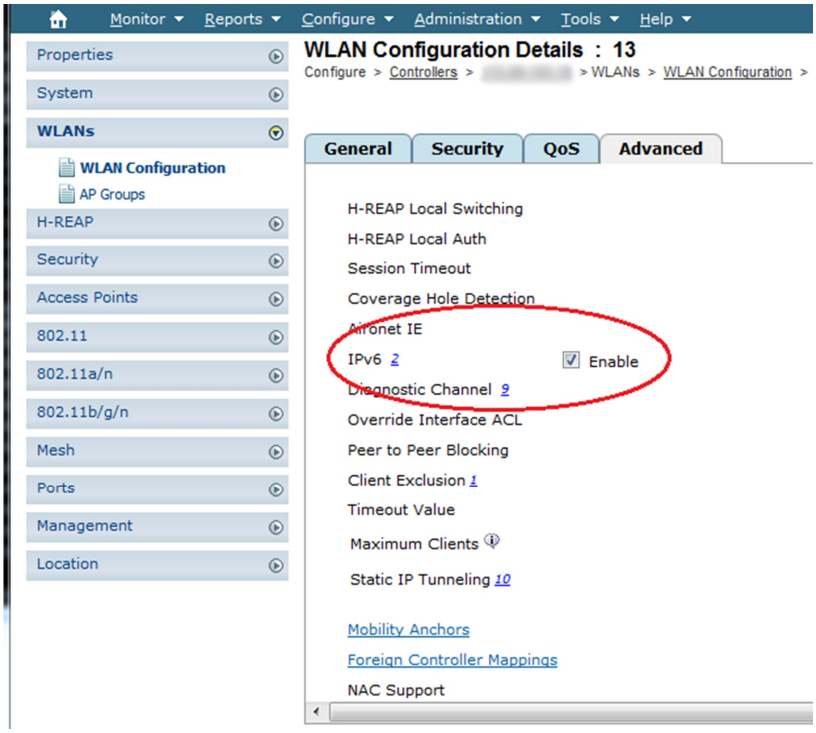
Esto-sääntöjen teon jälkeen IPv6 testi työasema -verkosta ei enää päässyt kirjautumaan testi DHCP-palvelimelle SSH-protokollalla, joten sääntöjen teko onnistui. Palomuurisääntöjen kirjoittaminen on hyvin samankaltaista IPv6- ja IPv4-protokollilla. Uuden säännön teon yhteydessä tarvitsee vain muistaa tehdä sama myös toisella protokollalla, joten huolellisuutta tarvitaan dual-stack-ympäristössä vielä entistä enemmän.

6.5 Kytkin

Kytkinverkolle ei tehty mitään muutoksia IPv6-kokeilujen aikana paitsi tietenkin pakolliset vlanien luonnit. Multicast-liikenteen toimivuus päätettiin jättää tämän opinnäytetyön ulkopuolelle, joten MLD snooping -ominaisuutta ei kokeiltu. Sen sijaan testin aikana laitteet oli kiinnitetty satunnaisesti vanhempiin ja uudempiin kytkimiin, jotka olivat joko HP Pro Curve- tai Cisco-merkkisiä kytkimiä. Hallinta IPv6-osoitteen antaminen onnistui ainoastaan Cisco Catalyst 2960-S -malleihin, mutta myös vanhemmat laitteet välittivät liikennettä ongelmitta.

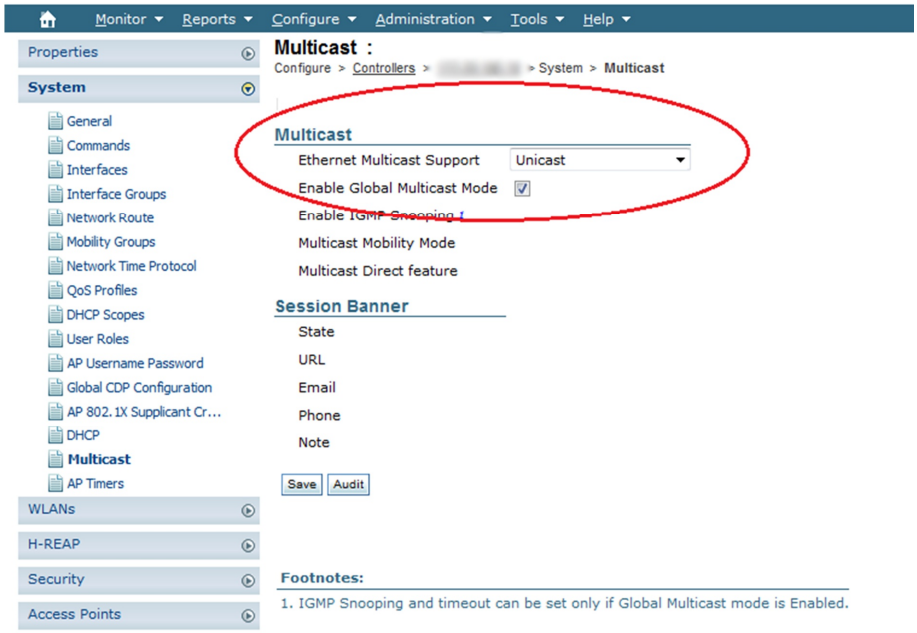
6.6 WLAN

WLAN-controllerina PHKK:lla on käytössä Ciscon 5500-sarjan tukiasemaohjain ja sekä Ciscon valmistamat Lightweight Access Point -tukiasemat. WLAN-controllereita ohjataan keskitetysti Ciscon Wireless Control Systemistä (WCS). Langattoman verkon toimivuus IPv6-protokollalla testattiin rakentamalla langaton testiverkko, jonka liikenne ohjattiin kytkimissä samaan verkkoon IPv6-testipalvelinten kanssa. Langattoman verkon asetukset muutettiin WCS-ohjelmistosta. Ensin tehtiin uusi langaton verkko, jonka toiminta testattiin IPv4-protokollalla. Tämän jälkeen laitettiin WLAN:n asetusten (jotka vaikuttavat yhteen WLAN-verkkoon) alta IPv6-täppä päälle (kuvio 19).



KUVIO 19. WLAN-asetusten määrittely IPv6-protokollalle

WLAN:n asetuksista laitettu täppä ei vielä saanut IPv6-liikennettä kulkemaan. WCS-hallintajärjestelmän huomautuksessa kehotettiin ottamaan multicast-liikenne käyttöön tukiasemien ja controllerin välillä. Tämä on välttämättömyys, että naapureiden etsintä, reititinmainostukset ja DHCPv6 toimisivat, koska kaikki ne toimivat multicast-osoitteilla. Seuraavaksi sallittiin multicast-liikenne tukiasemien ja kontrollerin välillä (kuvio 20).



KUVIO 20. WLAN-kontrollerin multicast asetukset

Multicast otettiin globaalisti käyttöön laittamalla täppä kohtaan ”Enable Global Multicast Mode”. Asetuksista löytyi seuraava kohta: ”Ethernet Multicast Support”, jolla voidaan määrittää WLAN-kontrollerille, tukeeko kytkinverkko multicast-liikennettä. Jos kohtaan valitsi ”Unicast”, muuttavat kontrolleri ja tukiasemat multicast-liikenteen ensin unicast-liikenteeksi ennen kuin lähettävät kytkinverkkoon. Kohdan toinen vaihtoehto olisi ollut ”Multicast”, jolloin multicast kulkisi sellaisenaan kytkinverkon lävitse. Testissä valittiin ”Unicast”, koska tukiasemat sijaitsevat erilaisten verkkojen takana, joten unicast-liikenne toimii varmemmin.

6.7 Linux-palvelut

Linux palveluita testattiin vanhalla työasemalla, jossa oli Intel Pentium 4 -prosessori ja 512 MB keskusmuistia. Työasemaan asennettiin 32-bittinen Scientific Linux 6.2. Sitten määritettiin verkkokortille asetukset. Verkkokortille asetettiin kiinteä IPv4- sekä IPv6-osoite. Verkkokortin asetukset löytyvät */etc/sysconfig/network-scripts/ifcfg-eth0*-tiedostosta. Tiedostoon määritettiin seuraavat asetukset:

DEVICE=eth0
IPADDR=a.a.a.a
NETMASK=b.b.b.b
GATEWAY=c.c.c.c
DNS1=d.d.d.d
IPV6INIT=yes
IPV6ADDR=2001:708:410:xx8::y

Verkkokortin asetusten muutosten jälkeen täytyy verkkoadapteri käynnistää uudestaan, jotta asetukset tulevat voimaan. Verkkokortti käynnistetään uudelleen komennolla: *service network restart*. Verkkokortin uudelleen käynnistyksen jälkeen tarkistettiin *ifconfig* –komennolla, että asetukset tulivat voimaan. Verkkokortille ei annettu mitään oletusreittiä, vaan annettiin reitittimen mainostaa oikeaa oletusreittiä. Lopuksi vielä pingattiin oletus reititintä varmistaakseen, että yhteys toimii.

Verkkoyhteyden toimiessa IPv4-osoitteella voidaan siirtyä seuraavaan vaiheeseen. Seuraavaksi päivitettiin asennusvaiheessa asennetut paketit uusimpiin versioihin. Tämä tehtiin komennolla *yum update*. Pakettien päivitys on suositeltava toimenpide, joka parantaa tietoturvaa.

Testiympäristöön haluttiin päästä kirjautumaan etänä, jolloin SSH-palvelu otettiin käyttöön. Ensin muutettiin muutama tietoturva-asetus sshd-palvelussa. Sshd-palvelun asetustiedot löytyvät tiedostosta: */etc/ssh/sshd_config*. Tiedostoon tehtiin seuraavat muutokset:

permitRootLogin no
PermitEmptyPasswords no
X11Forwarding no

PermitRootLogin rivi määrittää, että pääkäyttäjällä (Linuxissa root) ei voi kirjautua etänä. Monet hyökkääjät yrittävät kirjautua käyttäen root-käyttäjää, jolla on tietokoneeseen täydet oikeudet. PermitEmptyPasswords rivi määrittää, että sallitaanko etänä kirjautuminen käyttäjiltä, joilla ei ole salasanaa. X11Forwarding rivillä sallitaan tai kielletään graafisen työpöytäympäristön käyttäminen SSH-yhteyden ylitse. Tämä estetään, koska graafista työpöytäympäristöä ei ole asennettu ollenkaan. Muutosten jälkeen pitää palvelu käynnistää uudelleen komennolla: *service sshd restart*. Tässä vaiheessa huomattiin, että sshd-palvelu ei ole käynnistynyt itsestään käynnistyessä.

Seuraavaksi tarkistettiin *chkconfig*-komennolla, onko sshd-palvelu määritetty käynnistymään bootissa. Testiympäristössä tämä ei ollut oletuksena käynnistyvissä ohjelmissa. Sshd-palvelu lisättiin käynnistyvien palveluiden joukkoon komennolla *chkconfig sshd on*. Myös seuraavat muutokset tehtiin:

chkconfig NetworkManager off
chkconfig network on

Näillä muutoksilla muutettiin oletuksena ollut NetworkManager-palvelu ympäristössä paremmin toimivaan network-palveluun. Network-palvelun toiminta testattiin käynnistämällä kone uudelleen komennolla: *shutdown -r now*.

Etäkirjautuminen haluttiin sallia vain kahdesta verkosta, jotka ovat tietohallinnon hallussa. Tämä tehtiin sallimalla TCP-yhteydet porttiin 22 vain kahdesta verkosta. Iptables -palomuuripalvelun asetukset ja palomuurisäännöt löytyvät tiedostosta: */etc/sysconfig/iptables*. Tiedostosta poistettiin seuraava rivi, joka sallii yhteydet mistä tahansa lähdeosoitteesta:

-A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT

Tiedostoon lisättiin seuraavat rivit:

-A INPUT -m state --state NEW -m tcp -p tcp -s a.a.a.a/bb --dport 22 -j ACCEPT

-A INPUT -m state --state NEW -m tcp -p tcp -s c.c.c.c/bb --dport 22 -j ACCEPT

Tämän jälkeen täytyy palomuuripalvelu käynnistää uudelleen, jotta päivitetyt säännöt tulevat voimaan. Tämä tehdään komennolla *service iptables restart*. Palomuurisäännön toimivuus testattiin kokeilemalla kirjautua koneelle d.d.d.d/bb verkosta, jota ei lisätty sallittuihin. Tästä verkosta kirjautuminen ei onnistunut, mutta molemmista sallitusta onnistui hyvin.

6.7.1 DHCP-palvelu

Scientific Linux -testiympäristöön asennettiin DHCP-palvelu komennolla *yum install dhcp*. Paketin asennuksen jälkeen DHCP-palvelun konfiguraatio tiedosto

on ilmestynyt tiedostoon: /etc/dhcp/dhcpd.conf. Tämä tiedosto koskee IPv4:n DHCP-palvelun määrityksiä. Dhcpd.conf tiedostoon tehtiin seuraavat muutokset:

```
option domain-name "domain.name";
option domain-name-servers ns1.domain.name;

default-lease-time 600;
max-lease-time 7200;

authoritative;

subnet a.a.a.a netmask b.b.b.b {
range c.c.c.c d.d.d.d;
option routers e.e.e.e;
option domain-name-servers f.f.f.f;
}
```

Option domain-name ja *option domain-name-servers* määrittelee globaaleiksi aliverkoista riippumattomat asetukset. IP-osoitteiden lease-time jätettiin oletukseksi. Rivi *authoritative* otettiin kommentista pois, koska tällöin palvelin kieltää käyttäjiä käyttämästä muita osoitteita, kuin DHCP-palvelun konfiguraatioon on määritetty. Lopuksi määritettiin aliverkko a.a.a.a, jossa myös itse palvelin sijaitsi. DHCP-palvelun toiminta IPv4-osoitteilla testattiin ja todettiin toimivaksi edellä mainituilla asetuksilla.

Seuraavaksi DHCP-palveluun haluttiin ottaa käyttöön myös IPv6-osoitteiden jakaminen. Kun yum-pakettienhallinnalla asennettiin DHCP-paketti, asentui automaattisesti myös DHCPD6-palvelu, joka jakaa IPv6-osoitteita. DHCPD6-palvelu on oikeasti sama palvelu, mutta sitä ajetaan eri prosessissa. DHCPD6-palvelun konfiguraatiotiedosto löytyy samasta kansiosta, eli polusta */etc/dhcpd/dpchd6.conf*. Tiedostoon tehtiin seuraavat muutokset:

```
option dhcp6.domain-search “domain.name";

subnet6 2001:708:410:xx8::/64 {
    range6 2001:708:410:xx8::yy 2001:708:410:xx8::zz;
    option dhcp6.name-servers 2001:708:410:xx8::vv;
}
```

Option dhcp6.domain-search -rivillä annettiin domain nimi. Subnet6 määrittely vastaa IPv4-puolen DHCP:n aliverkkojen määrittelyä. Aliverkolle määriteltiin alue, josta jaetaan osoitteita ja nimipalvelimen osoite. Oletusreititintä ei voi tällä

DHCP-palvelimen versiolla jakaa, joten annoimme reitittimen mainostaa oletusreittiä.

Näillä määrittelyillä palvelu lähti käyntiin, mutta testi työasema ei saanut silti IPv6-osoitetta DHCP-palvelimelta. Ongelman syyksi löytyi ip6tables-palomuuri palvelimessa. DHCP-palvelu sallittiin kirjoittamalla */etc/sysconfig/ip6tables* -määritystiedostoon seuraava rivi:

-A INPUT -p udp --dport 547 -j ACCEPT

Asetus rivillä sallitaan UDP-liikenne porttiin 547, jota DHCPv6 käyttää. Client-pään portti olisi 546. Tämän jälkeen palvelu täytyi uudelleen käynnistää komennolla: *service ip6tables restart*. DHCPv6 toimi tämän jälkeen hyvin.

6.7.2 DNS-palvelu

DNS-palvelu asennettiin pakettienhallinnalla komennolla: *yum install bind*. Asennuksen jälkeen sallittiin iptables-palomuurissa molemmista testiverkoista verkoista DNS-kyselyt. Tämä tehtiin kirjoittamalla */etc/sysconfig/iptables* -konfiguraatiotiedostoon seuraava rivi:

-A INPUT -p udp --dport 53 -s a.a.a.a/bb -j ACCEPT

Tämän jälkeen palomuuripalvelu käynnistettiin uudelleen komennolla: *service iptables restart*. Tämän jälkeen muokattiin DNS-palvelun asetuksia tiedostosta: */etc/named.conf*. Tiedostoon tehtiin seuraavat muutokset:

```
listen-on port 53 { 127.0.0.1; a.a.a.a; };
listen-on-v6 port 53 { ::1;  fe80::z:z:z:z; 2001:708:410:xx8::y;
};
allow-query     { localhost; b.b.b.b/cc;  fe80::/64;
2001:708:410:xx8::/64; 2001:708:410:xx7::/64; };

zone "domain.name" IN {
        type master;
        file "domain.name.db";
        allow-update { none; };
};

zone "a.a.a.in-addr.arpa" IN {
        type master;
        file "a.a.a.db";
```

```
        allow-update { none; };
};

zone "b.b.b.in-addr.arpa" IN {
        type master;
        file "b.b.b.b.db";
        allow-update { none; };
};
```

Listen-riveillä kerrotaan, mitä osoitteita ja mistä portista halutaan kuunnella. Näille riveille lisättiin käytössä olevat IP-osoitteet. Palveluun määritettiin heti aluksi myös IPv6-osoitteet. Allow-query määrittelee, mistä verkoista tulleisiin kyselyihin vastattaan. Tähän kohtaan tuli kaikki käytössä testiympäristössä käytössä olleet verkot. Zone-määrittelyillä määriteltiin mitkä alueet ovat sisäisiä DNS-alueita. Zone-tietueiden määrittelyyn käytettiin malli konfiguraatiota pohjalla, muuttaen nimet ja tiedostonimet sopimaan tähän testiympäristöön. Alueiden määrittelytiedostojen sijaintia ei muutettu oletuksesta, joten ne löytyivät /var/named -hakemistosta. Tähän hakemistoon luotiin named.conf -tiedostossa määritellyt tiedostot: a.a.a.a.db, b.b.b.b.db ja domain.name.db.

Kaikkiin .db zonen määrittelytiedostoihin lisättiin seuraava alku:

```
$TTL    86400
@       IN      SOA     domain.name     domain.name.(
                2012030502      ;Serial
                3600            ;Refresh
                1800            ;Retry
                604800          ;Expire
                86400           ;Minimum TTL
)
                IN      NS      ns1.domain.name.
```

Nämä ovat pakollisia tietoja jokaisen zonen alussa. $TTL kertoo kuinka monta sekuntia kyseisen tiedoston määrittelyt ovat voimassa. SOA (Start of Authority Record) -rivi määrittelyineen on pakollinen, jossa kerrotaan tämän tiedoston sarjanumero (yleensä vvvvkkppxx –muodossa, jossa xx on kasvava järjestysnumero), refresh-rivi kertoo kuinka usein muut nimipalvelimet varmistavat tietojen oikeellisuuden, retry-rivi määrittää kuinka usein toinen nimipalvelin yrittää kysyä uudelleen refresh-laskurin mentyä nollaan. Expire-rivillä määritellään minkä ajan päästä muut nimipalvelimet eivät enää saa käyttää tätä tietoa. Minimum TTL -rivillä määritellään kuinka pitkän ajan muut

nimipalvelimet voivat kertoa käyttäjille että osoitetta ei löydy, mikäli sitä ei ole kyseisessä tiedostossa. SOA-tietueen jälkeen kerrotaan nimipalvelimen nimi. (RFC1035 1987, 18)

DNS-palvelussa käytetään hyväksi periyttämisominaisuutta, jolla voidaan määritellä osoitteen alkuosa tai nimen loppuosa. Esimerkiksi /etc/named.conf -tiedostossa määritelty zone: *a.a.a.a.in-addr.arpa* periyttää kyseiseen zoneen verkon a.a.a.a, jolloin tietokannassa voidaan kertoa ainoastaan viimeiset numerot. Mikäli periyttämistä halutaan muuttaa kesken zonen määrittelyn, täytyy se tehdä tällaisella rivillä zonen määrittelyssä: *$ORIGIN x.x.x.x.x.x.x.x.x.x.x.x.x.x.x.x.ip6.arpa.* IPv6-maailmassa voidaan periyttää jokaisen merkin kohdalta, koska pisteet ovat jokaisen merkin välissä.

SOA-tietueen määrittelyn jälkeen määritellään tietueet. A (Address) -tietue määrittää nimestä IPv4 osoitteeksi kääntämisen, kun taas AAAA-tietue määrittää nimestä IPv6-osoitteeksi kääntämisen. PTR (Pointer) -tietue määrittää IP-osoitteesta käänteisesti nimen selville. Alla esimerkit jokaisesta tietueesta:

```
ns1         IN    A       a.a.a.a
ns1         IN    AAAA    2001:708:410:xx8::y
10          IN    PTR     ns1.domain.name.
y.y.y.y.y.y.y.y.y.y.y.y.y.y.y.y          IN    PTR
ns1.domain.name.
```

Esimerkissä A- ja AAAA -tietueet ovat määritetty samassa tiedostossa, jossa ns1:n loppuun periytetään domain.name. PTR-rivit ovat eri tiedostoissa, koska toinen määrittelee IPv4:sta ja toinen IPv6:sta. 10-alkuiselle riville periytetään alku a.a.a. IPv6-riville periytetään alku: *8.x.x.x.0.1.4.0.8.0.7.0.1.0.0.2*. Tämä osoite käännettynä normaaliin esitystapaan on: 2001:708:410:xxx8.

Työssä ei lisätty muita omia tietueita. Tietueiden toimivuus testattiin ensin palvelimelta paikallisesti ja tämän jälkeen työasemalta, johon oli määritetty kyseinen palvelin nimipalvelimeksi. Lopuksi vielä testattiin, että hakeeko palvelin juurinimipalvelimilta osoitteita. Kaikki testit toimivat muuten hyvin, mutta juurinimipalvelimilta kysyttäessä oli noin 2000ms viive, koska todellista IPv6-yhteyttä juurinimipalvelimille ei ollut.

6.8 Testaushavainnot ja johtopäätökset

Testaukset menivät ehkä jopa odotettua paremmin. Kaikki kriittisimmät laitteet saatiin toimimaan. Alla taulukossa 8 on kerrottu lyhyesti tarvittavat muutokset laitteittain ja taulukon alla on tarkemmat selitykset muutoksista.

TAULUKKO 8. Tarvittavat muutokset laitekohtaisesti

Laite	Tarvittavat muutokset
Reititin	Ohjelmistopäivitys ja laajat konfiguraation muutokset
Palomuuri	Yksinkertaiset konfiguraation muutokset ja palomuurisääntöjen kopiointi
Kykin	Laitevaihtoja, jos halutaan täysi tuki, mutta nykyisillä pärjää ilman konfiguraatiomuutoksiakin.
WLAN	Konfiguraation muutokset, tulevaisuudessa lisää ominaisuuksia tulevalla ohjelmistopäivityksellä
Linux –palvelin	IPv6-osoitteen konfigurointi
DHCP-palvelu	Ohjelmistopäivitys ja nykyisten konfiguraatioiden kopiointi IPv6-osoitteille
DNS-palvelu	Uusien IPv6-tietueiden luonti

Aluksi testattiin DHCP- ja DNS-palveluiden toiminta. Tähän työhön otettiin vain kaikista yleisin malli kummastakin palvelusta, koska toinen henkilö teki opinnäytetyön palvelinmaailmasta, johon kuului muun muassa Microsoftin Windows Server 2008 R2:een kuuluva DNS-palvelin. ISC:n Linuxille tehdyt DHCP- ja DNS-palvelut toimivat koko testin ajan luotettavasti, joskin DNS-palvelu oli melko hidas. Hitaus johtui siitä, että palvelimella oli globaali IPv6-osoite, jolloin palvelin yritti käyttää IPv6-osoitetta juurinimipalveluista kyselyihin, mutta yhteyttä ulkomaailmaan IPv6-protokollalla ei ollut. DNS-palvelun omien tietueiden kyselyt toimivat ripeästi. DHCP-palvelu toimi koko

testin ajan luotettavasti. Testiympäristön perusteella ISC:n DNS- ja DHCP-palveluiden käyttöä voidaan jatkaa siirryttäessä IPv6-protokollaan.

Reitittimien vanhassa ohjelmistoversiossa oli PHKK:n verkkoa ajatellen suuria puutteita IPv6-ominaisuuksissa, joten ennen kuin mitään tehtiin, jouduttiin reitittimien ohjelmisto päivittämään. Ohjelmistopäivityksen jälkeen reitittimen ominaisuuksiin kuuluivat kaikki halutut IPv6-ominaisuudet. Reitittimen toiminta oli moitteetonta koko testin ajan ohjelmistopäivityksen jälkeen, joten nykyisillä reitittimillä voidaan turvallisin mielin siirtyä IPv6-protokollaan.

Palomuureista testiin pääsi ainoastaan sisäinen palomuurimoduuli FWSM. Sisäinen palomuuri ei vaadi muuta kuin access-listojen kopioinnin IPv4-säännöistä IPv6-sääntöihin. Kun dual-stack-ympäristö on saatu toimimaan tuotantoon, tulee juurikin palomuurisääntöjen pitäminen ajan tasalla molemmilla protokollilla olemaan suurin haaste dual-stack-ympäristössä. Ulkoverkon reunalla olevat Ciscon ASA -palomuurit näyttäisivät olevan konfiguroimista vailla valmiita IPv6-ympäristöön. Testaaminen jätettiin pois ulkoverkon IPv6-yhteyden puuttuessa.

Kytkimien kehittyneitä multicast-ominaisuuksia ei ollut mahdollisuutta testata tämän opinnäytetyön puitteissa. Mikäli kytkinten halutaan tukevan IPv6-tietoturvaominaisuuksia tai MLDv2:sta täytyisi tehdä laitehankintoja. Langaton järjestelmä kykenee välittämään IPv6-liikennettä, mutta muutoin langaton järjestelmä ei ole IPv6-yhteensopiva. Langattomassa järjestelmässä onkin etusijalla, että päätelaitteet voivat käyttää IPv6-protokollaa.

7 YHTEENVETO

Tämän opinnäytetyön tavoitteena oli selvittää, millaisia muutoksia PHKK:n tietoverkko vaatii, jotta voitaisiin turvallisin mielin ottaa uusi protokolla tuotantoverkon käyttöön. Opinnäytetyön pohjalta voidaan todeta, että PHKK:n nykyisissä runkolaitteissa on päivityksen jälkeen riittävät ominaisuudet ottaa tarvittaessa IPv6-protokollaa käyttöön dual-stack-tekniikalla. DHCP-palvelin vaati uudemman version ISC:n DHCP-palvelusta. Muut testatut laitteet saatiin toimimaan pelkillä konfiguraatioiden eli asetusten muutoksilla. Kytkimet vaatisivat fyysisten laitteiden vaihtoja, jotta saataisiin uudesta protokollasta kaikki hyödyt, mutta nykyisellääänkin kytkimet toimivat IPv6-protokollan kanssa ongelmitta.

Testien perusteella IPv6-protokollasta saatiin myös hyötyjä irti. Osoitteistus on helpompaa, kun voidaan käyttää vain yhden kokoisia verkkoja joka tarkoitukseen ja vlanien numerot saadaan sidottua paremmin IPv6-osoitteisiin. Nopeuseroja ei huomattu protokollien välillä. Dual-stack-tekniikaan nojautuva siirtymäaikakauden pituutta on vaikea ennustaa. Kun IPv4-protokolla voidaan ajaa alas ja käyttää pelkästään IPv6-protokollaa, työn määrä putoaa taas normaaliin mitä se oli IPv4-protokollan aikakaudella. NAT-tekniikasta päästään myös eroon IPv6-protokollaan siirtymisen yhteydessä.

Kun PHKK:ssa aletaan siirtyä tuotantoverkoissa IPv6-protokollaan, täytyy työ aloittaa reitittimistä ja palomuureista. Seuraavaksi DHCP-palvelun täytyy olla kunnossa. Ulkoverkon IPv6-tuki kuuluu myös ensimmäiseen vaiheeseen. DNS-palveluihin tulee tehdä AAAA-teitueita sitä mukaa kun palvelut alkavat tukea IPv6-protokollaa. Verkkolaitteista viimeisenä päivityslistalla voidaan pitää langatonta järjestelmää ja VPN-palvelua.

IPv6-protokollaan siirtyminen on työläs ja hidas prosessi, mutta se on välttämätöntä tehdä joka paikassa, jossa ollaan yhteydessä Internetiin. Mitä nopeammin työn aloittaa ja siirtymävaiheen saa päälle, sitä vähemmän on laitteita muutettavana, sillä Internetiin kytkettyjen laitteiden määrä kasvaa koko ajan kovaa vauhtia. IPv6-protokollasta ei vielä ole oikeata käytännön hyötyä, mutta pian palveluita on saatavilla enemmän IPv6-protokollalla kuin IPv4-protokollalla.

IPv6-protokollan käyttöönotto on myös imagollinen kysymys, ja yrityksen tietotekniikkaosastosta tulee ammattimaisempi kuva kun ollaan ottamassa ensimmäisten joukossa uutta teknologiaa käyttöön.

LÄHTEET

Desmeules, R. 2007. Cisco Self-Study: Implementing IPv6 Networks (IPV6). 3. painos. Indianapolis: Cisco Press.

Douglas, E. C. 2002. TCP/IP. Jyväskylä: Gummerrus.

Hakala, M. & Vainio, M. 2005. Tietoverkon rakentaminen. Jyväskylä: Docendo Finland Oy.

Bieringer, P. 2009. Linux IPv6 HOWTO [viitattu 8.3.2012] Saatavissa: http://tldp.org/HOWTO/Linux+IPv6-HOWTO/

Cisco. 2010. Cisco AnyConnect VPN Client Administrator Guide V. 2.0 [viitattu 16.4.2012]. Saatavissa: http://www.cisco.com/en/US/docs/security/vpn_client/anyconnect/anyconnect20/administrative/guide/admin.pdf

Cisco. 2011. NAT64—Stateless versus Stateful [viitattu 5.4.2012]. Saatavissa: http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6553/white_paper_c11-676277.html

CSC – Tieteen tietotekniikan keskus. 1998. ARPANET [viitattu 27.1.2012]. Saatavissa: http://www.nic.funet.fi/index/FUNET/history/internet/fi/arpanet.html

Huston, G. 2012. IPv4 Address Report [viitattu 23.2.2012]. Saatavissa: http://www.potaroo.net/tools/ipv4/index.html

RFC 5214. 2008. Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) [viitattu 16.4.2012]. Saatavissa: http://www.rfc-editor.org/rfc/rfc5214.txt

RFC 4380. 2006. Teredo: Tunneling IPv6 over UDP through Network Address Translations (NATs) [viitattu 16.4.2012]. Saatavissa: http://www.rfc-editor.org/rfc/rfc4380.txt

RFC 4291. 2006. IPv6 Addressing Architecture [viitattu 15.3.2012]. Saatavissa: http://www.rfc-editor.org/rfc/rfc4291.txt

RFC 1035. 1987. Domain names – Implementation and specification [viitattu 8.3.2012]. Saatavissa: http://www.rfc-editor.org/rfc/rfc1035.txt

Suomen virallinen tilasto (SVT). 2011. Tieto- ja viestintätekniikan käyttö. Helsinki: Tilastokeskus [viitattu 27.1.2012]. Saatavissa: http://www.stat.fi/til/sutivi/2011/sutivi_2011_2011-11-02_tie_001_fi.html

Wikipedia. 2012. Session Layer [viitattu 30.1.2012]. Saatavissa: http://en.wikipedia.org/wiki/Session_layer

Žorž, J & Steffann, S. 2010. Requirements For IPv6 in ICT Equipment. RIPE NCC [viitattu 17.4.2012]. Saatavissa: http://www.ripe.net/ripe/docs/ripe-501